INFORMATION SECURITY IN THE FEDERAL GOVERNMENT: ONE YEAR INTO THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 16, 2004

Serial No. 108–167

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

94–838 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

CONTENTS

INFORMATION SECURITY IN THE FEDERAL GOVERNMENT: ONE YEAR INTO THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

TUESDAY, MARCH 16, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:17 p.m., in room 2247, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) Presiding.

Present: Representative Putnam.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Chip Walker and Shannon Weinberg, professional staff members; Juliana French, clerk; Suzanne Lightman, fellow; Adam Bordes, minority professional staff member; and Cecelia Morton, minority office manager.

Mr. PUTNAM. Good afternoon. A quorum being present on this rainy Tuesday and the sound system back up and running, the Subcommittee on Technology, Information Policy, Intergovermental Relations and the Census will come to order.

Good afternoon and welcome to another important hearing on cybersecurity. This is the first oversight hearing conducted by the subcommittee on IT security this year.

Last year, we learned a great deal about threats, vulnerabilities, new technologies and new strategies for addressing the important issue of information security. Since our last hearing on this topic, the only thing that has really changed is the urgency of the threat.

While I believe that it may be fair to say that there might be more discussions taking place about these issues, the time for discussion and debate now yields to a more important requirement for action. Every month virus and worm attacks are becoming more prevalent and more malicious. One recent report placed the worldwide mitigation costs for the month of February 2004, at $83 billion. Some say that number is overinflated. So let's say that it's off by half. That's still a staggering number.

The cyber threat poses some very unique and difficult challenges. Our infrastructure and government systems can be attacked from anywhere, at any time. We know that various terrorist groups are very sophisticated and becoming more so each day, not to mention government-sponsored attacks. Our government has taken dra-

matic steps to increase our physical security, but protecting our information networks has not progressed commensurately, either in the public or private sectors. DHS is really just getting its feet on the ground in this arena. While I acknowledge the efforts of the National Cyber Security Division, I will reiterate my concern that we are collectively not moving fast enough to protect the American people and the U.S. economy from the very real threats that exist today.

The privacy and security of the public remain at risk. The economic damage being done to our economy is significant. The magnitude of this clearly is what makes this hearing so important, because governmentwide we are still failing to adequately secure our networks. Government must be the leader. We must set the standard, and we must do it now. The oversight by this subcommittee will be commensurate with the threat: ever increasing and aggressive.

In December of last year, the subcommittee released the 2003 Federal Computer Security Score Card. It was the 4th year that Federal agencies were graded, following the process begun by former Congressman Steve Horn. This past scorecard for the first time based grades on the criteria established by the Federal Information Security Management Act [FISMA].

Chairman Davis, through his FISMA legislation as part of the E-Government Act of 2002, laid the groundwork for better security and better reporting for the governments's computer systems. This year's grades were based on the FISMA compliance reports that the agencies provided to Congress and OMB in September of last year. OMB has worked hard to advance computer security at all the Federal agencies. I would also like to thank the GAO for their invaluable help in preparation of these grades.

This year is an important grading year because, for the first time, we can accurately compare the agencies to a previous year because the grading elements provide an apples-to-apples comparison.

This year overall the Federal Government received a grade of D. That's a modest increase over the F the government received last year.

For the first time, two agencies, the Nuclear Regulatory Commission and the National Science Foundation received A's.

Fourteen agencies have increased their grades this year, although a couple actually slid backward.

Only five agencies—five agencies—in the Federal Government have completed reliable inventories of their critical IT assets, leaving 19 without reliable inventories. This is troubling considering we are 4 years into this process and we still have far too many agencies with incomplete inventories.

How can you secure what you do not know you have? How can you claim to have completed a certification and accreditation process absent a reliable inventory of your assets?

The IGs of three agencies—DOD, Veterans Affairs and Treasury—did not submit reports in a timely manner. This represents a serious problem. I must stress the IG component of this equation is critically important. The independent verification is vital and particularly in light of the fact that there were significant dif-

ferences between many of the agencies and their IG's. Seven agencies had differences of two grades or more with their IGs.

Fourteen agencies are still below a C, and eight received failing grades.

As we worked on these grades, there were some overriding themes that became apparent for the agencies with good grades versus those with poor grades: a full inventory of their critical IT assets; they identified critical infrastructure and mission critical systems; a strong incident identification and reporting procedure; tight controls over contractors; strong plans of actions and milestones that serve as guides for finding and eliminating security weaknesses.

The Nuclear Regulatory Commission and the National Science Foundation should be commended for their outstanding scores, as well as the Social Security Administration and the Department of Labor for their B pluses. And while DHS has a failing grade this year, we recognize the difficult reorganization that took place and we expect significant improvement next year.

To assist agencies, I have requested that each of the 24 graded agencies come to meet with staff to discuss their grade. So far, staff has met with 14; and the results are very encouraging. We have seen a great deal of enthusiasm and willingness to do the work necessary. The agencies have also expressed gratitude for the opportunity to discuss the work they are doing and the grades with the subcommittee.

I am encouraged that OMB, in the recently released FISMA report and during Clay Johnson's testimony 2 weeks ago, stressed that there was an increased determination to hold agencies accountable for implementing FISMA. There is some clarification that I will seek today in something that is written in the OMB report. The report on page 13 says the following: "while awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. This issue requires the Federal Government to think of security in a new manner. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy and significantly endangers the ability of agencies to safeguard their IT investments."

While I agree that IT security is a collective responsibility, the language I referred to seems to indicate that no one person will be held accountable. I disagree. This chairman and this subcommittee will seek accountability of the highest agency official responsible for information technology investments to insure that IT security is baked into the investment decisionmaking process, consistent with the law as established in the Clinger-Cohen Act.

I have already initiated a process, working with Chairman Davis, to amend the Clinger-Cohen Act to explicitly identify information security as a required element of the IT investment management oversight and decisionmaking process within every agency of the Federal Government. The grade of D for the Federal Government simply is not acceptable.

Frankly, one of the continuing obstacles to progress is that too many people still view information security as a technology issue. This is a management and governance issue and must be accounted for in every business case and in implementation of a Federal enterprise architecture. This is the responsibility of all stakeholders, and the silo walls must come down with this and other transformation efforts to employ collaborative solutions that will provide increased safety and protection for the American people and the U.S. economy.

I welcome and applaud the increased oversight being employed by the Office of Management and Budget through the use of existing tools and business case evaluation. I particularly applaud the recent announcement that OMB will not approve agency expenditures for IT development and modernization projects until they have sufficiently demonstrated that their existing information technology assets are secure.

Working together as partners in progress, we will continue to be vigilant in our efforts to achieve the security of the information networks that support the mission activities of the Federal Government and protect the information assets that they contain.

Many cybersecurity technologies offered in today's marketplace can serve as safeguards and countermeasures to protect agencies' IT infrastructures. To assist agencies in identifying and selecting such technologies, I have asked GAO to categorize specific technologies according to the functionality they provide and describe what the technologies do, how they work, and their reported effectiveness. GAO is releasing this report today, and I want to thank them for their work and effort in producing this document. I read it on the plane up here, and it's outstanding. It is information security for dummies, Congressmen and bureaucrats; and I found it extremely helpful. Had I had that GAO report when I first became chairman, it would have knocked the learning curve down a bit, but it was very helpful.

I would like to welcome all of our witnesses here today. I want to thank you for your time, and I look forward to your testimony.

[The prepared statement of Hon. Adam H. Putnam follows:]

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
Congressman Adam Putnam, Chairman

OVERSIGHT HEARING

March 16, 2004

"Information Security in the Federal Government: One Year into the Federal Information Security Management Act."

STATEMENT BY ADAM H. PUTNAM, CHAIRMAN

This is the first oversight hearing conducted by this Subcommittee on IT security this year. Last year, we learned much about threats, vulnerabilities, new technologies and new strategies for addressing the important issue of information security. Since our last hearing on this topic, the only thing that has really changed is the urgency of the threat. While I think it may be fair to say that there might be more discussions taking place about these issues, the time for discussion and debate now yields to a more important requirement for ACTION. Every month virus and worm attacks are becoming more prevalent and more malicious. One recent report placed the worldwide mitigation costs for the month of February 2004 at $83 billion. Some might say that number is over inflated... but even if it's off by half, the number is still staggering.

The cyber threat posses some very unique and difficult challenges. Our infrastructure and government systems can be attacked from anywhere... at any time. We know that various terrorist groups are very sophisticated...and becoming more so each day, not to mention government sponsored attacks. Our government has taken very dramatic steps

to increase our physical security, but protecting our information networks has not progressed commensurately...either in the public...or private sector. DHS is really just getting its feet on the ground in this arena, and while I acknowledge the efforts of the National Cyber Security Division, I will reiterate my concern that we are "collectively" not moving fast enough to protect the American people and the U. S. economy from the very real threats that exist today.

The privacy and security of the public remains at risk. The economic damage being done to our economy is significant. The magnitude of this – clearly -- is what makes this hearing so important, because government-wide we still are failing to adequately secure our networks. Government must be the leader, we must set the standard and we must do it now. The oversight by this Subcommittee will be commensurate with the threat: Ever increasing and aggressive.

In December of last year, the Subcommittee released the 2003 Federal Computer Security Score Card. It was the 4th year that Federal agencies were graded following the process started by former Congressman Stephen Horn. This past scorecard, for the first time, based grades on the criteria established by the Federal Information Security Management Act (FISMA).

Chairman Tom Davis, through his FISMA legislation as part of the historic E-Government Act of 2002, has laid the groundwork for better security and better reporting for the government's computer systems. This year's grades were based on the FISMA compliance reports that the agencies provided to Congress and the Office of Management and Budget in September of last year. OMB has worked hard to advance computer security at all the Federal agencies and we have consulted OMB on the development of the scorecard. I would also like to thank the GAO for their invaluable help in preparation of these grades. This year is an important grading year because for the first time we can accurately compare the agencies to a previous year because the grading elements provided an apples-to-apples comparison. .

- This year overall the Federal Government gets a grade of D. That's a modest increase over the F the government received last year.

- For the first time, two agencies (The Nuclear Regulatory Commission and the National Science Foundation) have received A's.

- 14 agencies have increased their grades this year, although a couple actually went backwards.

- Only five agencies have completed reliable inventories of their critical IT assets leaving 19 without reliable inventories. This is very troubling considering we are four years into this process and still we have far too many agencies with incomplete inventories. How can you secure what you don't know you have? How can you claim to have completed a certification and accreditation process absent a reliable inventory of your assets...?

- The IGs of three agencies (DoD, Veterans Affairs, and Treasury) did not submit independent reports in a timely manner and that is a serious problem. I must stress the IG component of this equation is critically important. The independent verification is vital and particularly in light of the fact that there were significant differences between many of the agencies and their IGs. 7 agencies had difference of two grades or more with their IGs.

- 14 agencies are still below a C and eight received failing grades.

As we worked on these grades, there were some overriding themes that became apparent for the agencies with good grades vs. those with poor grades.

- A full inventory of their critical IT assets.
- Identified critical infrastructure and mission critical systems.
- A strong incident identification and reporting procedures.
- Tight controls over contractors.
- Strong plans of actions and milestones that serve as guides for finding and eliminating security weaknesses

The Nuclear Regulatory Commission and the National Science Foundation should be commended for their outstanding scores, as well as the Social Security Administration and the Department of Labor for their B pluses. And, while DHS had a failing grade we recognize the difficult reorganization that took place and we expect significant improvement next year.

To assist agencies, I have requested that each one of the 24 graded agencies come and meet with my staff to discuss their grade. So far, we have met with 14 agencies and the results are encouraging. We have seen a great deal of enthusiasm and willingness to do the hard work necessary. The agencies have also expressed thanks for the opportunity to discuss the work that they are doing and the grades with the Subcommittee.

I am encouraged that OMB, in the recently released FISMA report, and during Clay Johnson's testimony two weeks ago, stressed that there is an increased determination to hold agencies accountable for implementing FISMA. However, there is some clarification that I will seek today in something that was written in the OMB report. The report on page 13 says the following:

"While awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. This particular issue requires the Federal government to think of security in a new manner. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments."

While I certainly agree that IT security is certainly a collective responsibility the language I referred to seems to indicate that no one person can be held accountable. I

disagree. This Chairman and this Subcommittee will seek accountability of the highest agency official responsible for information technology investments to insure that IT Security is baked into the investment decision making process, consistent with the law as established by the Clinger-Cohen Act. In fact, I have already initiated a process, working with Chairman Davis, to amend the Clinger-Cohen Act to explicitly identify information security as a required element of the IT investment management oversight and decision making process within every agency of the federal government. The grade of D for the Federal Government is simply not acceptable.

Quite frankly, one of the continuing impediments to progress is that too many people still view information security as a technology issue. This is a management and governance issue and must be accounted for in every business case and in implementation of a federal enterprise architecture. This must be the responsibility of all stakeholders and the silo walls must come down with this and other transformation efforts to employ collaborative solutions that will provide increased safety and protection for the American people and the U. S. economy.

I welcome and applaud the increased oversight being employed by the Office and Management and Budget through the use of existing tools and business case evaluation. I especially applaud the recent pronouncement that OMB will not approve agency expenditures for IT development and modernization projects until they have sufficiently demonstrated that their existing information technology assets are secure. Working together as "partners in progress", we will continue to be vigilant in our efforts to achieve the security of the information networks that support the mission activities of the federal government, and protect the information assets that they contain.

To assist agencies in identifying and selection such technologies, I have asked GAO to categorize specific technologies according to the functionality they provide and describe what the technologies do, how they work and their reported effectiveness. GAO is releasing this report today and I want to thank them for their work and effort in producing this important product

I would like to welcome all our witnesses here today. Thank you for your time and I look forward to your testimony.

###

Mr. PUTNAM. I ask unanimous consent to insert in the record, the statement of my ranking member, the gentleman from Missouri, Mr. Clay. Without objection, show it done.

We will move directly into testimony.

All of you are old hands at this. You understand the light process, and we certainly appreciate your summarizing your statements.

Please rise and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. I indicate for the record that all the witnesses responded in the affirmative.

I would like to introduce our first witness, Robert Dacey. Mr. Dacey is currently Director of Information Security Issues at the U.S. General Accounting Office. I thought that we changed that. Has that passed the Senate yet? Don't you have a new name?

Mr. DACEY. I'm not sure quite yet.

Mr. PUTNAM. Everybody is waiting on the Senate.

His responsibilities include evaluating information systems, security and Federal agencies and corporations, assessing the Federal infrastructure for managing information security, evaluating the Federal Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats, and identifying best security practices at leading organizations and promoting their adoption by Federal agencies.

You are always a great asset as a witness to this subcommittee, and you are recognized. Welcome.

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. DACEY. Mr. Chairman, I am pleased to be here today to discuss the Federal Government's efforts to implement FISMA. As you requested, I will briefly summarize my written statement.

Since 1997, we have identified information security as a governmentwide high-risk issue. Congress has demonstrated their concern through ongoing hearings on information security and enactment of reform legislation. This subcommittee has played a very active role in addressing Federal information security challenges, including the grades you referred to in your opening statement which are based on a broad range of information included in the FISMA reports.

Based on our recent analysis of audit results and on reported FISMA information for 24 of the largest agencies, the Federal Government has made progress but continues to face significant information security risks to its critical operations, information and assets.

The first year FISMA reports provide important comparative data on information security performance measures and certain new information. The reports identify progress and highlight several challenges including the following.

No. 1, while reported performance measures generally increase, there continued to be a wide variance among the agencies.

No. 2, IG's reported less than half of agencies had complete system inventories now required by FISMA.

No. 3, reported systems with certification and accreditations continued to increase to 62 percent and systems with controls tested to 64 percent. However, both IG evaluations and our own ongoing review have identified efficiencies in the CNA processes, such as lack of control testing and outdated risk assessments. Also, as additional systems are certified and accredited and controls tested, it is likely that additional deficiencies will be identified.

No. 4, over half of agency systems do not have tested contingency plans, an essential step in ensuring that critical systems can continue to operate in the event of unexpected interruptions such as a cyber or physical attack.

No. 5, as a result of new OMB reporting requirements, IG's identified challenges in agencies' processes for remediating identified deficiencies which are key to ensuring that significant weaknesses are addressed in a timely manner and receive appropriate resources.

And, No. 6, we noted opportunities to improve the usefulness of reported measures included in FISMA reports included independent validation of reported information to ensure that such information is reliable.

In its fiscal year 2003 report to Congress, OMB concluded that the Federal Government has made significant strides in identifying and addressing longstanding problems, but the challenging weaknesses remain. In particular, the report notes several government-wide findings such as progress against milestones and lack of clear accountability for ensuring security of information and systems.

The report also presents a plan of action that OMB is pursuing with agencies to close the gaps and improve security. NIST also has taken a number of actions to develop FISMA-required system risk levels and corresponding minimum security standards and to improve Federal information security. However, according to NIST, current and future funding constraints could negatively impact its work in this area. Further, Mr. Chairman, as you noted in your opening statement, we released today our report on current cybersecurity technologies that are available to Federal agencies.

In summary, through the continued emphasis on information security by the Congress, the administration, agency management and the audit community, the Federal Government has seen improvements in its information security. Achieving significant and sustainable results will likely require agencies to institutionalize programs and processes that prioritize and routinely monitor and manage their information security efforts and provide information to facilitate day-to-day management of information security throughout the agency as well as verify the reliability of reported performance information.

Mr. Chairman, this concludes my statement. I'd be happy to answer any questions that you have.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 1:00 p.m. EST
Tuesday, March 16, 2004

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-04-483T

March 16, 2004

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-04-483T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Goverment Reform

INFORMATION SECURITY

Continued Efforts Needed To Sustain Progress in Implementing Statutory Requirements

Why GAO Did This Study

For many years, GAO has reported on the widespread negative impact of poor information security within federal agencies and has identified it as a governmentwide high-risk issue since 1997. Legislation designed to improve information security was enacted in October 2000. It was strengthened in December 2002 by new legislation, the Federal Information Security Management Act of 2002 (FISMA), which incorporated important new requirements.

This testimony discusses

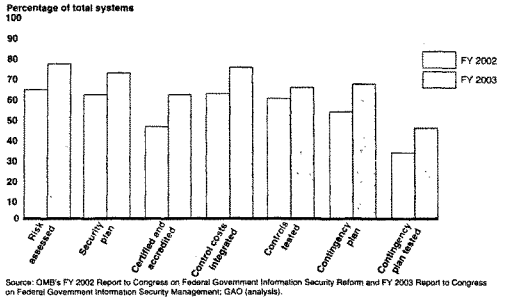
- the Office of Management and Budget's (OMB) recent report to the Congress required by FISMA on the government's overall information security posture,
- the reported status of efforts by 24 of the largest agencies to implement federal information security requirements,
- opportunities for improving the usefulness of performance measurement data, and
- progress by the National Institute of Standards and Technology (NIST) to develop related standards and guidance.

What GAO Found

OMB reports significant strides in addressing long-standing problems, but at the same time cites challenging weaknesses that remain. One governmentwide weakness OMB emphasizes is a lack of understanding—and therefore accountability—on the part of agency officials regarding their responsibilities for ensuring the security of information and systems. The report presents a plan of action to close these gaps through both management and budgetary processes.

Fiscal year 2003 FISMA data showed that, overall, the 24 federal agencies reported increasing numbers of their systems met the information security requirements represented by key OMB performance measures. For example, of the total number of systems reported by these agencies, the reported number assessed for risk climbed from 65 percent to 78 percent, those having a contingency plan jumped from 55 to 68 percent, and those authorized for processing following certification and accreditation rose from 47 to 62 percent (see chart). However, reported results varied widely among individual agencies, with some reporting that less than half of their systems met certain requirements. Further, GAO noted opportunities to improve the usefulness of reported performance management data, including independent validation of these data and completion of system inventories.

Reported Performance Measurement Data for Selected Information Security Requirements for 24 Large Federal Agencies



Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

NIST made progress in developing security-related standards and guidance required by FISMA. These include standards to categorize systems according to potential impact in the event of a security breach and recommended controls for such systems. However, according to NIST, current and future funding constraints could threaten its information security work.

www.gao.gov/cgi-bin/getrpt?GAO-04-483T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts by federal departments and agencies and the administration to implement requirements of the Federal Information Security Management Act of 2002 (FISMA).[1] For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences.[2] Further, since 1997, we have identified information security as a governmentwide high-risk issue in reports to the Congress—most recently in January 2003.[3]

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, in October 2000 the Congress passed and the President signed into law the Government Information Security Reform provisions (commonly known as GISRA) to strengthen information security practices throughout the federal government.[4] With GISRA expiring in November 2002, FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies by GISRA. FISMA added important new requirements, such as mandating that the National Institute of Standards and Technology (NIST) develop minimum information security requirements for information systems.

In my testimony today, I will summarize the federal government's overall information security progress and challenges as discussed in the Office of Management and Budget's (OMB) report to the Congress on fiscal year 2003 FISMA implementation released on March 1, 2004.[5] I will also discuss the reported status of efforts by 24 of the largest federal agencies to implement federal information security requirements, as well as opportunities for improving the usefulness of agency-reported FISMA performance measurement data.[6] I will then discuss actions being taken by NIST in meeting its FISMA requirements to develop information-security-related standards and guidance.

---

[1] *Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002,* P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

[2] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices,* GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

[3] U.S. General Accounting Office, *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures,* GAO-03-121 (Washington, D.C.: January 2003).

[4] *Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001,* P.L.106-398, October 30, 2000.

[5] Office of Management and Budget, *FY 2003 Report to Congress on the Federal Government Information Management,* March 1, 2004.

[6] These 24 departments and agencies are the Departments of Agriculture, Commerce, Defense (DOD), Education, Energy, Health and Human Services, Homeland Security (DHS), Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, Office of Personnel Management, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. These agencies exclude the Federal Emergency Management Agency, which is now within the new DHS. DHS also incorporated components of other agencies, including the U.S. Coast Guard and U.S. Customs Service, that were formerly within the Departments of Transportation and the Treasury, respectively.

In conducting this review, we reviewed and summarized the fiscal year 2003 FISMA reports for 24 of the largest federal agencies and their inspectors general (IGs). In addition, we reviewed standards and guidance issued by NIST pursuant to its FISMA responsibilities and discussed the progress of these efforts with NIST officials. We also reviewed and summarized OMB's March 2004 report to the Congress on FISMA implementation. We did not validate the accuracy of the data reported by the agencies or OMB, but did analyze the IGs' fiscal year 2003 FISMA reports to identify any issues related to the accuracy of FISMA-reported information. We performed our work from October 2003 to March 2004, in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2003 report to the Congress, OMB notes that the federal government has made significant strides in identifying and addressing long-standing problems, but that challenging weaknesses remain. In particular, the report notes several governmentwide findings, such as limited progress against governmentwide information security milestones and a lack of clear accountability for ensuring security of information and systems. The report also presents a plan of action that OMB is pursuing with agencies to close those gaps and improve the security of federal information and systems. Planned actions include prioritizing agencies' information technology (IT) spending to resolve security weaknesses and improving the federal government's incident prevention and management capabilities to respond to the increasing number and potential impact of threats and vulnerabilities.

Fiscal year 2003 data reported by the 24 large agencies for a subset of OMB's performance measures show increasing numbers of systems meeting the statutory information security requirements represented by these measures compared with fiscal year 2002. For example, the total number of systems that had been assessed for risk increased by 13 percentage points to 78 percent. Other reported key measures, such as the percentage of systems with up-to-date security plans, also showed increases ranging from 4 to 15 percentage points.

Agencies' fiscal year 2003 FISMA reports showed that performance measures for many agencies have increased, but there are wide variances among the agencies. For example, compared with last year's results, 17 agencies reported increases in the percentage of systems authorized for processing after certification and accreditation—a process that OMB considers an important information security

quality control.[7] However, only 6 agencies reported that they had authorized 90 to 100 percent of their systems, and 11 of the remaining 18 agencies reported that they had authorized less than half of their systems. Moreover, the IGs' evaluations, as well as our own ongoing review, have identified deficiencies in agencies' certifications and accreditations, such as lack of control testing and outdated risk assessments. We also noted several opportunities to improve the usefulness of reported performance management data, including independent validation of reported information, completion of system inventories, and providing performance information based on the relative importance or risk of the systems.

For its part, NIST has taken a number of actions to develop security-related standards and guidance required by FISMA. These include the issuance of standards to categorize federal information and information systems according to levels of potential impact on organizational operations, assets, or individuals, should a breach of security occur. However, according to NIST, current and future funding constraints could affect its information security and critical infrastructure protection work, including providing guidance and other assistance to agencies to improve their information security.

Background

Our recent analyses of audit results for federal agencies showed improvement, but continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. The significance of these weaknesses led GAO to recently conclude that information security was a material weakness in our audit of the federal government's fiscal year 2003 financial statements.[8] Audits also identified instances of similar types of weaknesses in non-financial systems, which continue to receive increased audit coverage in response to FISMA requirements. Weaknesses continued to be reported in each of the six major areas of general

[7] *Certification* is the comprehensive evaluation of the technical and nontechnical security controls of an IT system that provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. This management approval, or *accreditation*, is the authorization of an IT system to process, store, or transmit information that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation decision is based on the implementation of an agreed-upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it. Agencies are required to reaccredit their systems prior to a significant change in processing, but at least every 3 years (more often where there is a high risk and potential magnitude of harm).

[8] U.S. General Accounting Office, *Fiscal Year 2003 U.S. Government Financial Statements: Sustained Improvement in Federal Financial Management Is Crucial to Addressing Our Nation's Future Fiscal Challenges*, GAO-04-477T (Washington, D.C.: March 3, 2004).

controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, a principal focus of FISMA, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, also addressed by FISMA, which ensures that computer-dependent operations experience no significant disruptions.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high. The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Congress and the administration have established specific information security requirements in both law and policy to help protect the information and information systems that support these critical operations.

FISMA Permanently Authorizes and Strengthens Information Security Requirements

On October 30, 2000, Congress passed GISRA, which was signed into law and became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and was consistent with existing information security guidance issued by OMB[9] and NIST,[10] as well as audit and best practice guidance issued by GAO.[11] Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA permanently authorized and strengthened GISRA's information security program, evaluation, and reporting requirements. Like GISRA, FISMA assigns specific responsibilities to agency heads, chief information officers (CIO), and IGs. It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security; and reviewing at least annually, and approving or disapproving, agency information security programs. FISMA continues to delegate OMB responsibilities for national security systems to the Secretary of Defense and the Director of Central Intelligence.

Overall, FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;

[9]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.
[10]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.
[11]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA also established a requirement that each agency develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

The law also requires an agency's CIO to designate a senior agency information security officer who, for the agency's FISMA-prescribed information security responsibilities, shall

- carry out the CIO's responsibilities;
- possess professional qualifications, including training and experience, required to administer the required functions;
- have information security duties as that official's primary duty; and
- head an office with the mission and resources to assist in ensuring agency compliance.

Under FISMA, each agency must continue to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national-security systems are to be performed by the agency IG or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

FISMA requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices, and compliance with FISMA's requirements. In addition, agency heads are required to annually report the results of their independent evaluations to OMB, except that to the extent an evaluation pertains to a national security system, only a summary and assessment of that portion of the evaluation is reported to OMB. OMB is also required to submit a report to the Congress no later than March 1 of each year on agency compliance with FISMA's requirements, including a summary of findings of agencies' independent evaluations. FISMA also requires the Comptroller General to periodically evaluate and report to Congress on (1) the adequacy and effectiveness of agency information security policies and practices and (2) implementation of FISMA requirements.

Other major FISMA provisions require NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST must also develop a definition of and guidelines concerning detection and handling of information security incidents; and guidelines, developed in conjunction with the Department of Defense and the National Security Agency, for identifying an information system as a national security system.

The law also assigned other information security functions to NIST, including

- providing technical assistance to agencies on such elements as compliance with the standards and guidelines and the detection and handling of information security incidents;
- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;
- developing and periodically revising performance indicators and measures for agency information security policies and practices;
- evaluating private-sector information security policies and practices and commercially available information technologies to assess potential application by agencies;
- evaluating security policies and practices developed for national security systems to assess their potential application by agencies; and
- periodically assessing the effectiveness of and revising, as appropriate, the NIST standards and guidelines developed under FISMA.

NIST is required to prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out its responsibilities under FISMA.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

On August 6, 2003, OMB issued its fiscal year 2003 FISMA reporting instructions and guidance on quarterly IT security reporting.[12] These instructions, which required agencies to submit their reports to OMB by September 22, 2003, essentially continued many of the reporting requirements established for GISRA, including performance measures introduced for fiscal year 2002 reporting under that law. The instructions also highlighted the more substantive changes introduced by FISMA. For example, OMB emphasized that FISMA applies to both information and information systems used by an agency and by its contractors or other organizations and sources that possess or use federal information or that operate, use, or have access to federal information systems. OMB also underscored that FISMA requires each agency to test and evaluate the effectiveness of the information security policies, procedures, and practices for each system at least annually.

OMB's fiscal year 2003 reporting instructions also emphasized the strong focus on performance measures and formatted these instructions to emphasize a quantitative rather than a narrative response. OMB also required agencies to provide quarterly updates for a key subset of these performance measures, with the first update due December 15, 2003. Measures within this key subset are the numbers of systems that have

- risk assessments and assigned levels of risk,
- up-to-date IT security plans,
- certifications and accreditations,
- security control costs integrated into their life cycles,
- security controls tested and evaluated in the last year,
- contingency plans, and
- contingency plans tested.

Further, OMB provided instructions for continued agency reporting on the status of remediation efforts through plans of action and milestones (POA&M). Required

[12]Office of Management and Budget, "*Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*," Memorandum for Heads of Executive Departments and Agencies, Joshua B. Bolten, Director, M-03-19, August 6, 2003.

for all programs and systems where an IT security weakness has been found, a POA&M lists the weaknesses and shows estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions. POA&Ms are to be submitted twice a year. In addition, agencies are to submit quarterly updates that show the number of weaknesses for which corrective action was completed on time (including testing), is ongoing and on track to be completed as originally scheduled, or has been delayed; as well as the number new weaknesses discovered since that last update.

Consistent with last year, OMB's fiscal year 2003 guidance continued to authorize agencies to release certain information from their POA&Ms to assist the Congress in its oversight responsibilities. Agencies could release this information, as requested, excluding certain elements, such as estimated funding resources and the scheduled completion dates for resolving a weakness.

Lastly, as part of IG FISMA reporting, OMB instructed the IGs to respond to essentially the same questions that the agencies were to respond to in their reports. The IG responses were to be based on the results of their independent evaluations, including agency progress in implementing and maintaining their POA&Ms, and any other work performed throughout the reporting period (such as financial statement or other audits). This year, OMB also asked the IGs to assess against specific criteria whether the agency had developed, implemented, and was managing an agencywide POA&M process. OMB noted that this assessment was critical because effective remediation of IT security weaknesses is essential to achieving a mature and sound IT security program and securing information and systems. Further, OMB identified this IG assessment as one of the criteria used in evaluating agencies under the Expanding E-Government Scorecard of the President's Management Agenda.

OMB also instructed the IGs to use the performance measures to assist in evaluating agency officials' performance. However, it did not request them to validate agency responses to the performance measures. Instead, as part of their independent evaluations of a subset of agency systems, IGs were to assess the reliability of the data for those systems that they evaluated.

OMB's Report to Congress Notes Progress and Challenges

In its *FY 2003 Report to Congress on Federal Government Information Security Management*, published this month, OMB concludes that the federal government has made significant strides in identifying and addressing long-standing problems, but that challenging weaknesses remain. Overall, the report discusses the steps taken by OMB and federal agencies to implement FISMA, details progress made in fiscal year 2003, and identifies IT security gaps and weaknesses. The report also presents a plan of action that OMB is pursuing with agencies to close these gaps and improve the security of federal information and systems. This plan is intended

to resolve information and security challenges through both management and budgetary processes.

OMB's report discussed four governmentwide findings:

1. *Agencies' Progress Against Governmentwide IT Security Milestones.* The President's fiscal year 2004 budget established three governmentwide goals to be met by the end of calendar year 2003. These goals and the progress reported against them were:

   - Goal 1 — As required by FISMA, all federal agencies are to have created a central remediation process to ensure that program and system-level IT security weaknesses, once identified, are tracked and corrected. In addition, each agency IG is to verify whether the agency has a process in place that meets criteria specified in OMB guidance. Based on IG responses to these criteria, OMB reported that each agency has an IT security remediation process, but that the maturity of these processes varies greatly. In particular, the report noted that for the 24 large agencies, only half have a remediation process verified by their IGs as meeting the necessary criteria.

   - Goal 2 — Eighty percent of federal IT systems are to be certified and accredited. OMB reported that many agencies are not adequately prioritizing their IT investments to ensure that significant IT security weaknesses are appropriately addressed. As a result, at the end of 2003, the reported percentage of systems certified and accredited had increased to 62 percent, but was still short of the goal. Related to this goal, the report noted that most security weaknesses can be found in operational systems that either have never been certified and accredited or whose certification and accreditation are out of date.

   - Goal 3 — Eighty percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment. OMB reported that agencies have made improvements in integrating security into new IT investments, but that significant problems remain, particularly in ensuring security of existing systems. As an example, the report provided results for the performance measure related to this goal, which showed that at the end of 2003, the percentage of systems that had integrated security into the lifecycle of the investment increased to 78 percent.

2. *Agency Progress Against Key IT Security Measures.* As the report highlights, because of GISRA and the OMB-developed performance measures, the federal government is now able to measure progress in IT security; and the Congress, OMB, the agencies, and GAO are able to track and monitor agency efforts against those measures. Noting agency progress, the report provides a table comparing results of 24 large federal agencies for key performance measures

for fiscal years 2001, 2002, and 2003. However, it also notes that further work is needed, and uses the area of contingency planning as an example, where only 48 percent of the systems had tested contingency plans. A comparison of reported overall results for fiscal year 2002 and 2003 is provided below in table 1.

Table 1: Comparison of Fiscal Year 2002 and Fiscal Year 2003 Performance Measurement Data for 24 Large Federal Agencies

	Total		Assessed for risk and assigned a level of risk		Up-to-date IT security plan		Processing authorized following certification/ accreditation		Security control costs integrated into system life cycle		Security controls tested and evaluated in the last year		Have a contingency plan		Contingency plan tested	
Year	FY02	FY03	FY02	FY03	FY02	FY03	FY02	FY03	FY02	FY03	FY02	FY03	FY02	FY03	FY02	FY03
Number of systems*	7,957	7,998	5,160	6,236	4,930	5,838	3,772	4,969	4,919	6,182	4,751	5,143	4,342	5,450	2,768	3,839
Percent of total systems			65	78	62	73	47	62	62	77	60	64	55	68	35	48
Difference from FY02 to FY03	+41 systems		+13 percentage points		+11 percentage points		+15 percentage points		+15 percentage points		+4 percentage points		+13 percentage points		+13 percentage points	

*Fiscal year 2002 totals include data for FEMA, which is now part of DHS.

Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

3. *IGs' Assessment of Agency Plan of Action and Milestones Process.* As mentioned in the discussion of goal 1, OMB requested that IGs assess against a set of criteria whether the agency had a robust agencywide plan of action process. OMB reported the overall results of this assessment for the 24 agencies, which showed that 8 had such a process; 4 did, but with improvements needed; 11 did not; and one did not submit a report (DOD).

4. *Lack of Clear Accountability for Ensuring Security of Information and Systems.* The report emphasizes that even with the strong focus of both GISRA and FISMA on the responsibilities of agency officials regarding security, there continues to be a lack of understanding, and therefore, accountability within the federal government. Issues that continue to be a concern include the following:

   - Agency and IG reports continue to identify the same IT security weaknesses year after year, some of which are seen as repeating material weaknesses.
   - Too many legacy systems continue to operate with serious weaknesses.

- As a result, there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development.

In further discussing this finding, the report concludes that these concerns must be addressed through improved accountability, that is, holding agency program officials accountable for ensuring that the systems that support their programs and operations are secure. Further, it emphasizes that ensuring the security of an agency's information and systems is not the responsibility of a single agency official or the agency's IT security office, but rather a responsibility to be shared among agency officials that support their operations and assets.

The report also outlines a plan of action to improve performance that identifies specific steps it will pursue to assist agencies in their IT security activities, promote implementation of law and policy, and track status and progress. These steps are:

- *Prioritizing IT Spending to Resolve IT Security Weaknesses.* OMB reports that it used information from agencies' annual FISMA reports and quarterly POA&M updates in making funding decisions for fiscal year 2004, as well as for fiscal year 2005 to address longer term security weaknesses. For example, agencies with significant information and system security weaknesses were directed to remediate operational systems with weaknesses prior to spending fiscal year 2004 IT development or modernization funds. Further, if additional resources are needed to resolve those weaknesses, agencies are to use those fiscal year 2004 funds originally sought for new development.
- *President's Management Agenda Scorecard.* To "get to green" under the Expanding E-Government Scorecard for IT security, agencies are required to meet the following three criteria: (1) demonstrate consistent progress in remediating IT security weaknesses; (2) attain certification and accreditations for 90 percent of their operational IT systems; and (3) have an IG-assessed and IG-verified agency POA&M process.
- *Fiscal Year 2004 OMB FISMA Guidance.* OMB plans to further emphasize performance measurement in next year's guidance. In particular, its focus will center on three areas: (1) evolving the IT security performance measures to move beyond status reporting to also identify the quality of the work done, such as determining both the number of systems certified and accredited and the quality of certification and accreditation conducted; (2) further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes, such as remediation and intrusion detection and reporting; and (3) providing additional clarity to certain definitions to eliminate interpretation differences within agencies and among agencies and IGs.
- *Threat and Vulnerability Response Process.* In response to the increasing number and potential impact of threats and vulnerabilities, OMB will continue to focus on

improving the federal government's incident prevention and management capabilities. Such improvements include an increased emphasis on reducing the impact of worms and viruses through more timely installation of patches for known vulnerabilities, and improved information sharing to rapidly identify and respond to cyber threats and critical vulnerabilities. OMB also notes the critical importance of agency business continuity plans to mitigating the impact of threats and vulnerabilities.

Finally, OMB's March 2004 report to the Congress identifies several other issues, and provides additional summary and agency-specific information. These include the following:

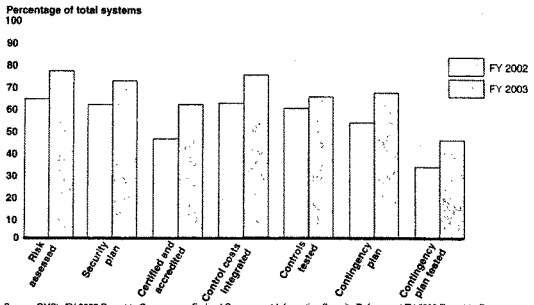
- As one of the changes or additions introduced by FISMA, a stronger emphasis is placed on configuration management. Specifically, FISMA requires each agency to develop specific system configuration requirements that meet its own needs and ensure compliance with them. According to the report, this provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Further, adequate ongoing monitoring and maintenance must accompany the establishment of such configuration requirements.
- Federal funding for IT security increased from $2.7 billion in fiscal year 2002 to $4.2 billion in fiscal year 2003. The report also continues to emphasize that, historically, a review of IT security spending and security results has demonstrated that spending is not a statistically significant factor in determining agency security performance. Rather, the key is effectively incorporating IT security in agency management actions and implementing IT security throughout the lifecycle of a system.
- The report appendixes provide an overview of the federal government's IT security program, a summary of performance by 55 small and independent agencies, and individual summaries for each of the 24 large agencies.

FISMA Reports Highlight Overall Increases in Performance Measures, But Individual Agency Results Vary Widely

Overall, fiscal year 2003 data reported by the agencies for a subset of OMB's performance measures show increasing numbers of systems meeting the requirements represented by these measures. For example, as shown in table 1, the reported percentage of systems authorized for processing following certification and accreditation increased from 47 percent for fiscal year 2002 to 62 percent for fiscal year 2003—an increase of 15 percentage points. In addition, the reported number of systems assessed for risk and assigned a level of risk increased by 13 percentage points from 65 percent for fiscal year 2002 to 78 percent for fiscal year 2003. Reported increases for other measures ranged from 4 to 15 percentage points. Figure 1 illustrates the reported overall status of the 24

agencies in meeting these requirements and the increases between fiscal years 2002 and 2003.

Figure 1: Reported Performance Measurement Data for Selected Information Security Requirements for 24 Large Federal Agencies



Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

This subset of performance measures highlights important information security requirements. However, agencies' FISMA reports also address other specific statutory requirements, regarding such elements as incident response capabilities, information security training, review of agency contractor operations and facilities, and remediation processes. The agency reports, as well as the IGs independent evaluations are intended to address all the FISMA requirements, and it is these reports and evaluations that your subcommittee reviewed in assigning agency grades for your December 2003 computer security report card.

The data and other information submitted for fiscal year 2003 FISMA reporting did show overall increases by many agencies for certain measures, but also that wide variances existed among the agencies. As discussed earlier, we did not validate the accuracy of the data reported by the agencies, but did analyze the IGs' fiscal year 2003 FISMA reports to identify issues related to the accuracy of this information. Also as discussed later, we noted opportunities to improve the usefulness of agency-reported data. Further, in considering FISMA data, it is important to note that as more systems are subject to the certification and accreditation process and periodically tested, it is probable that additional significant weaknesses will be identified; and until all systems have contingency plans that are periodically tested, agencies have limited assurance that they will

be able to recover from unexpected events. Summaries of results reported for specific requirements follow.[13]

Risk Assessment

As part of the agencywide information security program required for each agency, FISMA mandates that agencies assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of their information and information systems. OMB, through information security policy set forth in its Circular A-130,[14] also requires an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system.[15]

As defined in NIST's current draft revision of its *Risk Management Guide for Information Technology Systems*, risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level where risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.[16] Risk assessment is the first process in the risk management process, and organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its systems development life cycle. Our best practices work has also shown that risk assessments are an essential element of risk management and overall security program management, and are an integral part of the management processes of leading organizations.[17] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls.

To measure agencies' performance in implementing this requirement, OMB mandates that agencies' FISMA reports provide the number and percentage of systems that have been assessed for risk.

---

[13]Our summarization and categorization of agency-reported information included data provided for the OMB-prescribed performance measures. In several instances, agency reports either did not address or provide sufficient data for a question or measure. IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. In addition, the DOD IG did not submit an independent evaluation report that provided the required data for fiscal year 2003.

[14]Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130, Revised, Transmittal Memorandum No. 4, Appendix III, "Security of Federal Automated Information Resources" (Nov. 28, 2000).

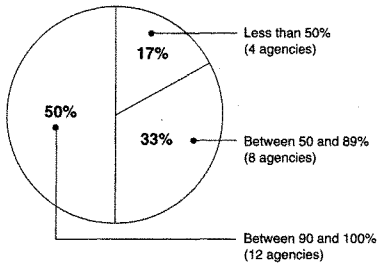
[15]OMB describes security requirements for both *general support systems* and *major applications*. A general support systems is defined as an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A major application is defined as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[16]National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Draft Special Publication 800-30 Rev A (January 2004).

[17]GAO/AIMD-98-68.

Reporting for this measure continued to show overall increases. Specifically, 14 of the 24 agencies reported an increase in the percentage of systems assessed for risk for fiscal year 2003 as compared with fiscal year 2002. Further, as illustrated in figure 2, 12 agencies reported that they had assessed risk for 90 to 100 percent of their systems for fiscal year 2003, and only 4 of the remaining 13 agencies reported that less than half of their systems had been assessed for risk (compared with 8 agencies for fiscal year 2002).

Figure 2: Percentage of Systems Assessed for Risk for Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Security Plans

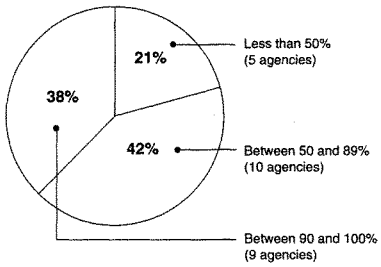
FISMA requires that agencywide information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. According to NIST security plan guidance, the purpose of these plans is to (1) provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements, and (2) delineate the responsibilities and expected behavior of all individuals who access the system. OMB Circular A-130 requires that agencies prepare IT system security plans consistent with NIST guidance, and that these plans contain specific elements, including rules of behavior for system use, required training in security responsibilities, personnel controls, technical security techniques and controls, continuity of operations, incident response, and system interconnection.[18]

[18]National Institute of Standards and Technology, *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18 (December 1998).

Agencies are also to update security plans as part of the cycle for reaccrediting system processing.

As a performance measure for this requirement, OMB requires that agencies report number and percentage of systems with up-to-date security plans. Agency data reported for this measure showed overall increases for fiscal year 2003, with a total of 9 agencies reporting up-to-date security plans for 90 percent or more of their systems compared with 7 agencies for fiscal year 2002. Further, of the remaining 15 agencies, only 5 reported that less than 50 percent of their systems had up-to-date security plans, compared with 9 agencies in 2002. Figure 3 summarizes overall fiscal year 2003 results.

Figure 3: Percentage of Systems with Up-to-Date Security Plans for Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Note: Total does not add to 100 percent due to rounding.

Certification and Accreditation

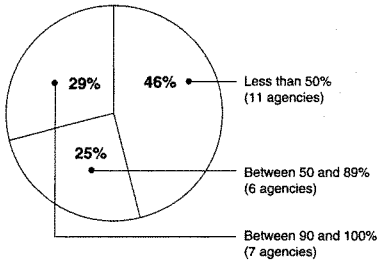
As part of its responsibilities under FISMA, OMB is required to develop and oversee the implementation of policies, principles, standards, and guidelines on information security. Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. NIST is currently in the process of updating its guidance for the certification and accreditation of federal systems (except for national

security systems).[19] This guidance is to be used in conjunction with other standards and guidance that FISMA requires NIST to issue—documents that, when completed, are intended to provide a structured yet flexible framework for identifying, employing, and evaluating the security controls in federal information systems.

Because OMB considers system certification and accreditation to be such an important information security quality control, for FISMA reporting, it requires agencies to report the number of systems authorized for processing after certification and accreditation.

Data reported for this measure showed overall increases for most agencies. For example, 17 agencies reported increases in the percentage of systems authorized compared with their percentages last year. In addition, 7 agencies reported that they had authorized 90 to 100 percent of their systems compared with only 3 agencies last year. However, 11 agencies reported they had authorized less than 50 percent of their systems, but this also indicated some improvement compared with the 13 agencies that reported less than 50 percent last year (which included 3 that reported none). Figure 4 summarizes overall results for the 24 agencies for fiscal year 2003.

Figure 4: Percentage of Systems during Fiscal Year 2003 that are Authorized for Processing after Certification and Accreditation



Source: Agency-reported data and GAO (analysis).

The results of the IGs' independent evaluations showed deficiencies in agencies' system certifications and accreditations, including instances in which certifications and accreditations were not were not current and controls were not tested. In addition, at the request of the House Committee on Government Reform

[19]National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Second Public Draft, Special Publication 800-37 (June 2003).

and your subcommittee, we are currently reviewing federal agencies' certification and accreditation processes. Preliminary results of our work indicate that the majority of the 24 large agencies reported that they are using NIST or other prescribed guidance for their system certifications and accreditations. However, our reviews of the certification and accreditation of selected systems at selected agencies identified instances where documentation did not show that specific criteria were always met. For example, we noted instances in which systems were accredited even though risk assessments were outdated, contingency plans were incomplete or untested, and control testing was not performed. Further, in some cases, documentation did not clearly indicate what residual risk the accrediting official was actually accepting in making the authorization decision. Unless agencies ensure that their certifications and accreditations meet appropriate criteria, the value of this process as a management control for ensuring information system security is limited, and agency reported performance data may not accurately reflect the status of an agency's efforts to implement this requirement.

Integration of Security Costs into the System Life Cycle

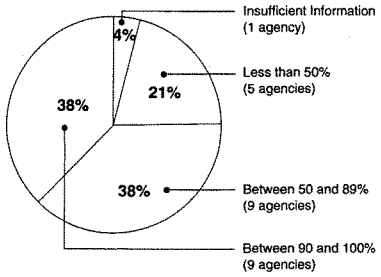
OMB requires that agencies' budget submissions specifically identify security costs as part of life-cycle costs for their IT investments and has provided criteria to be considered in determining such costs.[20] OMB also provided these security cost criteria in its FISMA guidance and required agencies to report their IT security spending, including those critical infrastructure protection costs that apply to the protection of government operations and assets. Among other questions related to including security costs in IT investments, OMB requires that the agencies report the number of systems that have security control costs integrated into their system life cycles.

Fiscal year 2003 reporting for this measure showed that agencies are increasingly integrating security control costs into the life cycle of their systems. Specifically, 15 agencies reported increases in the number of systems integrating security

[20]Criteria to be considered include the products, procedures, and personnel (federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Examples include costs for risk assessment; security planning and policies; certification and accreditation; specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security); authentication or cryptographic applications; education, awareness, and training; system reviews/evaluations (including security control testing and evaluation); oversight or compliance inspections; development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment; contingency planning and testing; physical and environmental controls for hardware and software; auditing and monitoring; computer security investigations and forensics; and reviews, inspections, audits and other evaluations performed on contractor facilities and operations. Agencies must also include the products, procedures, and personnel that have as an incidental or integral component a quantifiable benefit to IT security for the specific IT investment, such as configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; and systems administrator functions. For the security costs of application investments, agencies should also appropriately allocate the costs of networks, which may provide some or all of the necessary security controls for the associated applications.

costs, compared with the number reported last year. Also, as shown in figure 5, 9 agencies reported meeting this measure for 90 to 100 percent of their systems.

Figure 5: Percentage of Systems that Have Security Control Costs Integrated into the Life Cycle of their Systems for Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Note: Total does not add to 100 percent due to rounding.

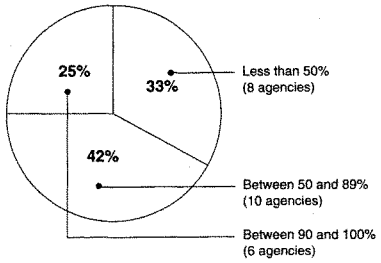
Security Control Testing and Evaluation

FISMA requires that agency information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency that depends on risk, but no less than annually. This is to include testing of management, operational, and technical controls of every information system identified in the FISMA-required inventory of major systems. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost-effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of program reviews is an additional source of information that can be considered along with control testing and evaluation in IG and our audits to help provide a more complete picture of the agencies' security postures.

As a performance measure for this requirement, OMB mandates that agencies report the number of systems for which security controls have been tested and

evaluated. Fiscal year 2003 data reported for this measure showed that a total of 15 agencies reported an increase in the overall percentage of systems being tested and evaluated. However, 8 agencies still reported that they had tested the controls of less than 50 percent of their systems (compared with 10 agencies last year) and only 6 of the remaining 16 agencies reported testing and evaluating the controls for 90 percent or more of their systems (compared with 4 agencies last year). Figure 6 shows the overall results for fiscal year 2003.

Figure 6: Percentage of Systems with Security Controls Tested during Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Contingency Plans

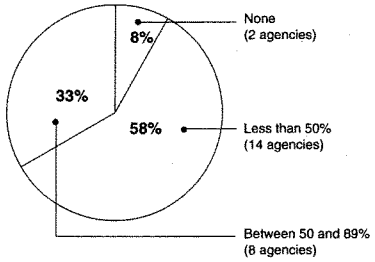
FISMA requires that agencies' information security programs include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities, in case usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, accidental loss of files, or major disaster. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations.

The testing of contingency plans is essential to determine whether they will function as intended in an emergency situation, and the frequency of plan testing will vary depending on the criticality of the entity's operations. The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers

will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

To show the status of implementing this requirement, OMB mandates that agencies report the number of systems that have a contingency plan and the number with contingency plans that have been tested. Agencies' reported fiscal year 2003 data for these measures showed that contingency planning remains a problem area for many agencies. Specifically, a total of 11 agencies report that less than half of their systems have contingency plans and of the remaining 13 agencies, only 6 have contingency plans for 90 to 100 percent of their systems. In addition, a total of 14 agencies reported that they had tested contingency plans for less than half of their systems, including 2 agencies that reported testing none. Figure 7 provides overall results for fiscal year 2003 contingency plan testing.

Figure 7: Percentage of Systems with Contingency Plans That Have Been Tested for Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Note: Total does not add to 100 percent due to rounding.

Security Training

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide training on information security to personnel with significant security responsibilities. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had

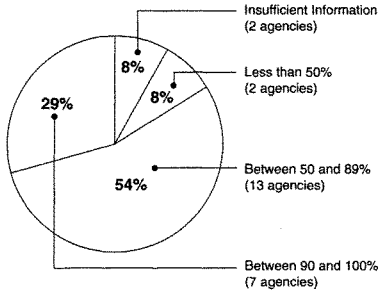
the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools.

As performance measures for FISMA training requirements, OMB has the agencies report the number of employees who received IT security training during fiscal year 2003 and the number of employees with significant security responsibilities who received specialized training.

Reported fiscal year 2003 data showed that 13 agencies reported that they provided security training to 90 to 100 percent of their employees and contractors compared with 9 agencies for fiscal year 2002. Of the remaining 11 agencies, only 3 reported that such training was provided for less than half of their employees/contractors, and 1 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, reported data showed increases since fiscal year 2002. For example, a total of 7 agencies reported training for 90 to 100 percent of their employees with significant security responsibilities (compared with 5 agencies last year), and of the remaining 17 agencies, only 2 reported providing training to less than half of such employees (compared with 10 for fiscal year 2002). Figure 8 provides overall results for fiscal year 2003.

Figure 8: Percentage of Employees with Significant Security Responsibilities Receiving Specialized Training during Fiscal Year 2003



Source: Agency-reported data and GAO (analysis).

Note: Total does not add to 100 percent due to rounding.

Incident Handling

Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect them before significant damage can be done. Accounting for and analyzing security problems and incidents are also effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. Problem and incident reports can, therefore, provide valuable input for risk assessments, help in prioritizing security improvement, and be used to illustrate risks and related trends in reports to senior management.

FISMA requires that agencies' information security programs include procedures for detecting, reporting, and responding to security incidents; mitigating risks associated with such incidents before substantial damage is done; and notifying and consulting with the FISMA-required federal information security incident center and other entities, as appropriate, including law enforcement agencies and relevant IGs. OMB information security policy has also required that system security plans ensure a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. In addition, NIST has provided guidance to assist organizations in establishing computer security incident-response capabilities and in handling incidents efficiently and effectively.[21]

OMB requires agencies to report several performance measures and other information for FISMA related to detecting, reporting, and responding to security incidents. These include the number of agency components with an incident handling and response capability, whether the agency and its major components share incident information with the Federal Computer Incident Response Center (FedCIRC)[22] in a timely manner, and the numbers of incidents reported. OMB also requires that agencies report on how they confirm that patches[23] have been tested and installed in a timely manner and whether they are a member of FedCIRC's Patch Authentication and Distribution Capability, which provides agencies with

[21]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 (January 2004).
[22]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention, and recognition for the federal government.
[23]A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered. Patch management is the process of effectively applying available patches.

information on trusted, authenticated patches for their specific technologies without charge.[24]

Agency-reported data showed that many agencies have established and implemented incident-response capabilities for their components. For example, 17 agencies reported that for fiscal year 2003, 90 percent or more of their components had incident handling and response capabilities (compared to 12 agencies for fiscal year 2002). Also, a total of 18 agencies reported that their components report incidents to FedCIRC either themselves or centrally through one group.

A total of 22 agencies reported that they confirm patches have been tested and installed in a timely manner. In contrast, of the 23 IGs that reported, 11 responded that the agency confirmed that patches have been tested and installed in a timely manner; 5 that the agency did but not consistently; and 6 that the agency did not (1 other IG did not provide sufficient data). A total of 19 agencies also reported that they were a member of FedCIRC's Patch Authentication and Distribution Capability.

In our September 2003 testimony, we discussed the criticality of the patch management process in helping to alleviate many of the challenges involved in securing computing systems from attack.[25] We also identified common practices for effective patch management found in security-related literature from several groups, including NIST, Microsoft,[26] patch management software vendors, and other computer-security experts. These practices included

- senior executive support of the process;
- standardized patch management policies, procedures, and tools;
- dedicated resources and clearly assigned responsibilities for ensuring that the patch management process is effective;
- current inventory of all hardware equipment, software packages, services, and other technologies installed and used by the organization;
- proactive identification of relevant vulnerabilities and patches;

[24]According to a DHS official, the department recently decided to terminate the Patch Authentication and Distribution Capability based on low levels of usage, negative agency feedback on its usefulness, and the cost to make significant upgrades. Further, many of its customers only used this service for patch notification, which can generally be obtained through vendors at no cost.
[25]U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Sep. 10, 2003).
[26]Microsoft Corporation, *Solutions for Security, Solutions for Management: The Microsoft Guide to Security Patch Management* (Redmond, WA: 2003).

- assessment of the risk of applying the patch considering the importance of the system to operations, the criticality of the vulnerability, and the likelihood that the patch will disrupt the system;
- testing each individual patch against various systems configurations in a test environment before installing it enterprisewide to determine any impact on the network;
- effective patch distribution to all users; and
- regular monitoring through network and host vulnerability scanning to assess whether patches have been effectively applied.

In addition to these practices, we identified several steps to be considered when addressing software vulnerabilities, including:

- deploying other technologies, such as antivirus software, firewalls, and other network security tools, to provide additional defenses against attacks;
- employing more rigorous engineering practices in designing, implementing, and testing software products to reduce the number of potential vulnerabilities;
- improving tools to more effectively and efficiently manage patching;
- researching and developing technologies to prevent, detect, and recover from attacks as well as to identify their perpetrators, such as more sophisticated firewalls to keep serious attackers out, better intrusion-detection systems that can distinguish serious attacks from nuisance probes and scans, systems that can isolate compromised areas and reconfigure while continuing to operate, and techniques to identify individuals responsible for specific incidents; and
- ensuring effective, tested contingency planning processes and procedures.

Security of Contractor-Provided Services

Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. Thus, as OMB emphasized in its fiscal year 2003 FISMA reporting guidance, agency IT security programs apply to all organizations that possess or use federal information or that operate, use, or have access to federal information systems on behalf of a federal agency. Such other organizations may include contractors, grantees, state and local governments, and industry partners. This underscores longstanding OMB policy concerning sharing government information and interconnecting systems: federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

As a performance measure for the security of contractor-provided security, OMB had the agencies report the number of contractor facilities or operations reviewed and to respond as to whether or not they used appropriate methods (such as audits or inspections and agreed-upon IT security requirements) to ensure that contractor-provided services for their programs and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

Fiscal year 2003 data reported for these measures showed that 10 of the 24 agencies reported that they had reviewed 90 to 100 percent of their contractor operations or facilities. Only 2 agencies reported having reviewed less than half of their contractor operations or facilities, and two others provided insufficient data for this measure. In addition, 22 agencies reported that they used appropriate methods to ensure that contractor-provided services are adequately secure and meet the requirements of FISMA. Of the remaining two agencies, one reported that it did not use appropriate methods and one reported partial compliance. Although these reported results indicate overall increases from fiscal year 2002, the IGs' evaluations provided different results. For example, although the IG evaluations did not always address these measures, 9 of the 15 IGs that did report showed that less than half of contractor operations or facilities were reviewed. Further, only 12 IGs reported that the agency used appropriate methods to ensure that contractor-provided services are adequately secure and meet the requirements of FISMA, while 7 reported that their agencies did not.

Plan of Action and Milestones

FISMA requires that agencies' information security programs include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. Further, a centralized process for monitoring and managing remedial actions enables the agency to identify trends, root causes, and entitywide solutions.

As discussed previously, as part of GISRA implementation, OMB began requiring that agencies report on the status of their remediation efforts through POA&Ms and quarterly updates. In addition, for fiscal year 2003 FISMA reporting, OMB had agency IGs assess whether the agency had developed, implemented, and was managing an agencywide plan of action and milestone process according to specific criteria, such as whether agency program officials and the CIO develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness; and whether the agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.

Overall, the IGs' responses to these criteria showed that many agencies still do not use the POA&M process to manage the correction of their information security weaknesses. For example, as part of monitoring the status corrective actions, 20 of the 23 IGs that reported responded that the agency CIO tracked POA&M data centrally on at least a quarterly basis, but only 12 reported that the CIO maintained POA&Ms for every system that has an IT weakness. Further, 14 IGs reported that their agency POA&M process did not prioritize IT security weaknesses to ensure that significant weaknesses are addressed in a timely manner and receive appropriate resources. Reported IG responses to these and other criteria are summarized in table 2.

Table 2: Summary of Inspector General Assessment of Agency POA&M Processes

	Inspector General Responses					
	Yes		No		Data not provided	
OMB reporting criteria	Number	(%)	Number	(%)	Number	(%)
Agency program officials have POA&Ms for every system they own and operate that has an IT security weakness	11	(48)	10	(43)	2	(9)
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress	14	(61)	8	(35)	1	(4)
Agency CIO has POA&Ms for every system it owns and operates that has an IT security weakness	12	(52)	10	(44)[1]	1	(4)
Agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis	20	(87)	3	(13)	0	(0)
POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses	14	(61)	8	(35)	1	(4)
System-level POA&Ms are tied directly to the system budget request through the IT business case to tie the justification for IT security funds to the budget process	10	(44)[1]	12	(52)	1	(4)
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms	18	(78)	5	(22)	0	(0)
The agency's POA&M process represents a prioritization of agency IT security weaknesses to ensure that significant weaknesses are addressed in a timely manner and receive appropriate resources	8	(35)	14	(61)	1	(4)

[1]Rounded up to total 100 percent.

Source: Agency Fiscal Year 2003 FISMA reports and GAO (analysis).

Opportunities Exist to Improve the Usefulness of Performance Measurement Data

Periodic reporting of performance measures tied to FISMA requirements and related analysis can provide valuable information on the status and progress of agency efforts to implement effective security management programs, thereby assisting agency management, OMB and the Congress in their management and oversight roles. However, several opportunities exist to improve the usefulness of such information as indicators of both governmentwide and agency-specific performance in implementing information security requirements. As discussed earlier, OMB plans to further emphasize performance measurement in next year's FISMA reporting guidance, including evolving measures to identify the quality of work performed, targeting IG efforts to assess key security processes, and clarifying certain definitions. In developing its guidance, OMB can consider how their efforts can help to address the following factors that lessen the usefulness of current performance measurement data:

- *Limited assurance of data reliability and quality.* The performance measures reported by the agencies are primarily based on self-assessments and are not independently validated. OMB did not require the IGs to validate agency responses to the performance measures, but did instruct them to assess the reliability of the data for the subset of systems they evaluate as part of their independent evaluations. Although not consistently addressed by all the IGs, some IG evaluations did identify problems with data reliability and quality that could affect agency performance data. For example, for the performance measure on the number of agency systems authorized for processing after certification and accreditation, 6 IGs indicated different results than those reported by their agencies for reasons such as out-of-date certifications and accreditations (systems are to be reaccredited at least every 3 years). Further, other IGs identified problems with the quality of the certifications and accreditations, such as security control reviews not being performed.

- *Accuracy of agency system inventories.* The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. Further, a complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. As mentioned, FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. However, according to their fiscal year 2003 FISMA reports, only 13 of the 24 agencies reported that they had completed their system inventories. Further, independent evaluations by IGs for 3 of these 13 agencies did not agree that system inventories were complete. In addition, although there was little change in the reported total number of systems shown for the 24 agencies

(an increase of only 41 systems from 7,957 systems for fiscal year 2002 to 7,998 systems for fiscal year 2003, large changes in individual agencies' total systems from year to year could make it more difficult to interpret changes in their performance measure results. For example, the total number of systems reported by the Department of Agriculture decreased by 55 percent from 605 for fiscal year 2002 to 271 for fiscal year 2003, which the department attributed, in large part, to its efforts to develop the FISMA-required inventory of major information systems. At the same time, all of the department's key performance measures increased, with some, such as systems assessed for risk, showing a large increase (from 18 percent for fiscal year 2002 to 72 percent for fiscal year 2003).

- *Limited Department of Defense data.* In interpreting overall results for the federal government, it is important to note that reported numbers include only a small sample of the thousands of systems identified by DOD. Attributing its size and complexity and the considerable lead time necessary to allow for the collection of specific metrics and the approval process by each service and agency, DOD determined that the collection of a sample of system and network performance metrics would effectively support its emphasis on network-centric operations and complement its overall information assurance security reporting. Obtaining OMB concurrence with this approach, DOD provided performance measurement data on a sample of 378 systems in its fiscal year 2003 FISMA report. As OMB reported in its fiscal year 2003 report to the Congress, DOD reported a total of 3,557 systems for the department—almost half of the combined total systems for the other 23 agencies. OMB also reported that DOD plans to report on all systems for the fiscal year 2004 reporting cycle. As a result, including performance data on all DOD systems for fiscal year 2004 could significantly affect the overall performance measurement results both for DOD and governmentwide.

- *Data are reported in aggregate, not according to system risk.* Performance measurement data are reported on the total number of agency systems and do not indicate the relative importance or risk of the systems for which FISMA requirements have been met. Reporting information by system risk would provide better information about whether agencies are prioritizing their information security efforts according to risk. For example, the performance measures for fiscal year 2003 show that 48 percent of the total number of systems have tested contingency plans, but do not indicate to what extent these 48 percent include the agencies' most important systems. Therefore, agencies, the administration, and the Congress cannot be sure that critical federal operations can be restored if an unexpected event disrupts service. As required by FISMA, NIST recently issued its *Standards for Security Categorization of Federal Information and Information Systems* to provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs and consistent reporting to OMB and the Congress on the adequacy and effectiveness of information security policies, procedures, and

practices.[27] These standards, which are discussed later in greater detail, would require agencies to categorize their information systems according to three levels of potential impact on organizations or individuals—high, moderate, and low—should there be a breach of security.

- *Refinement of Performance Measures Could Improve Quality of Analysis.* Refinement of performance measures can provide more useful information about the quality of agency processes. For example, as discussed earlier, GAO and the IGs have noted issues concerning the quality of the certification and accreditation process. Additional information reported on key aspects of certification and accreditation would provide better information to assess whether they were performed consistently. As also discussed earlier, OMB's fiscal year 2003 FISMA report to the Congress also identified the need to evolve performance measures to provide better quality information.

Status of NIST Efforts

Since FISMA was enacted in December 2002, NIST has taken a number of actions to develop required security-related standards and guidance. These actions include the following:

- In December 2003 it issued the final version of its *Standards for Security Categorization of Federal Information and Information Systems* (FIPS Publication 199). NIST was required to submit these categorization standards to the Secretary of Commerce for promulgation no later than 12 months after FISMA was enacted. The standards establish three levels of potential impact on organizational operations, assets, or individuals should a breach of security occur—**high** (severe or catastrophic), **moderate** (serious), and **low** (limited). These standards are intended to provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs, and consistent reporting to OMB and the Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
- Also in December 2003, it issued the initial public draft of its *Guide for Mapping Types of Information and Information Systems to Security Categories* (Special Publication 800-60). Required to be issued 18 months after FISMA enactment, this guidance is to assist agencies in categorizing information and information systems according to impact levels for confidentiality, integrity, and availability as provided in NIST's security categorization standards (FIPS Publication 199).

[27]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199, December 2003.

- In October 2003 it issued an initial public draft of *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) to provide guidelines for selecting and specifying security controls for information systems categorized in accordance with FIPS Publication 199. This draft includes baseline security controls for low and moderate impact information systems, with controls for high impact systems to be provided in subsequent drafts. This publication, when completed, will serve as interim guidance until 2005 (36 months after FISMA enactment), which is the statutory deadline to publish minimum standards for all non-national-security systems. In addition, testing and evaluation procedures used to verify the effectiveness of security controls are to be provided this spring in NIST's *Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems* (Special Publication 800-53A).

- In August 2003 it issued *Guideline for Identifying an Information System as a National Security System* (Special Publication 800-59). This document provides guidelines developed in conjunction with DOD, including the National Security Agency, to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements. Except for national security systems identified by FISMA, the Secretary of Commerce is responsible for prescribing standards and guidelines developed by NIST. DOD and the Director of Central Intelligence have authority to develop policies, guidelines, and standards for national security systems. The Director is also responsible for policies relating to systems processing intelligence information.

According to a NIST official, the agency has also made progress in implementing other FISMA requirements. For example, it is continuing to provide consultative services to agencies on FISMA related information security issues and has established a federal agencies security practices Web site to identify, evaluate, and disseminate best practices for critical infrastructure protection and security. In addition, it has established a Web site for the private sector to share nonfederal information security practices. NIST has continued an ongoing dialogue with the National Security Agency and the Committee on National Security Systems to coordinate and take advantage of the security work underway within the federal government.

FISMA also requires NIST to prepare an annual public report on activities undertaken in the previous year and planned for the coming year, to carry out its responsibilities. According to a NIST official, this report should be issued this month.

In addition to its responsibilities under FISMA, NIST has issued or is developing other information security guidance that supports this law. Along with its guidance on incident handling, building an information security awareness program, and draft guidance on both certification and accreditation and risk management, NIST has also issued *Security Metrics Guide for Information*

Technology Systems[28] and *Security Considerations in the Information System Development Life Cycle: Recommendations of the National Institute of Standards and Technology.*[29]

Current budget constraints may, however, affect NIST's future work. FISMA established new responsibilities for this agency and authorized an appropriation of $20 million for each fiscal year, 2003 through 2007. However, according to NIST, funding for the Computer Security Division, the organization responsible for FISMA activities, was reduced from last year, and this will affect this division's information security and critical infrastructure protection work.

In addition to the specific responsibilities to develop standards and guidance under FISMA, other information security activities undertaken by NIST include

- operating a computer security expert assist team (CSEAT) to assist federal agencies in identifying and resolving IT security problems;
- conducting security research in areas such as access control, wireless, mobile agents, smart-cards, and quantum computing;
- improving the security of control systems that manage key elements of the country's critical infrastructure; and
- performing cyber security product certifications required for government procurements.

The Cyber Security Research and Development Act also assigned information security responsibilities to NIST and authorized funding. These responsibilities include

- providing research grants to institutions of higher education or other research institutions to support short-term research aimed at improving the security of computer systems; growth of emerging technologies associated with the security of networked systems; strategies to improve the security of real-time computing and communications systems for use in process control; and multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.
- developing cyber security checklists (and establishing priorities for their development) that set forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the federal government.

[28]National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55 (July 2003).
[29]National Institute of Standards and Technology, *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64 (October 2003).

In summary, through the continued emphasis of information security by the Congress, the administration, agency management, and the audit community, the federal government has seen improvements in its information security. However, despite the apparent progress shown by increases in key performance measures, most agencies still have not reached the level of performance that demonstrates that they have implemented the agencywide information security program mandated by FISMA. If information security is to continue to improve, agency management must remain committed to these efforts and establish management processes that ensure that requirements are implemented for all their major systems, including new requirements to categorize their systems and incorporate mandatory minimum security controls. Performance measures will continue to be a key tool to both hold agencies accountable and provide a barometer of the overall status of federal information security. For this reason, it is increasingly important that agencies' monitoring, review, and evaluation processes provide the Congress, the administration, and agency management with assurance that these measures accurately reflect agency progress. Opportunities to provide this assurance and improve the usefulness of agencies' performance measurement data include IG validation of reported data, categorization of the data according to system risk levels, and refinement of the measures to provide more information about the quality of agency processes.

Achieving significant and sustainable results will likely require agencies to develop programs and processes that prioritize and routinely monitor and manage their information security efforts. Further, agencies will need to ensure that systems and processes are in place to provide information and facilitate the day-to-day management of information security throughout the agency, as well as to verify the reliability of reported performance information.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317 or Ben Ritt, Assistant Director, at (202) 512-6443. We can also be reached by e-mail at daceyr@gao.gov and rittw@gao.gov, respectively.

Other individuals making key contributions to this testimony included Larry Crosland, Mark Fostek, Danielle Hollomon, and Barbarol James.

(310522)

Mr. PUTNAM. Our next witness is Karen Evans.

In September 2003, Karen Evans was appointed by President Bush to be Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. Prior to joining OMB, Ms. Evans was Chief Information Officer at the Department of Energy and served as vice chairman of the CIO Council, the principal forum for agency CIOs to develop IT recommendations. Previously, she served at the Department of Justice as Assistant and Division Director for Information System Management. She is doing a great job over at OMB.

We're always delighted to have you join us and share your expertise with us. You are recognized.

STATEMENT OF KAREN EVANS, ADMINISTRATOR, ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Thank you.

Good afternoon, Mr. Chairman. Thank you for inviting me to speak about the status of the Federal Government's efforts to safeguard our information and systems. My remarks will focus on the findings of the OMB fiscal year 2003 FISMA report and the next steps to address our IT security challenges.

Earlier this month, OMB issued our third annual report to Congress on agency compliance with IT security requirements in law and policy. FISMA, like its predecessor, the Government Information Security Reform Act, continues to be a valuable tool in improving the state of Federal IT security, both the security of systems and promoting the protection of information.

The OMB FISMA report identifies IT security progress and weaknesses in fiscal year 2003. The report summarizes progress such as Federal performance against three governmentwide goals identified in the President's fiscal year 2004 budget. Agencies reported their progress against a key set of IT security performance measures. These measures reveal areas of the progress from fiscal year 2001 through 2003 as well as weaknesses.

Agency IG reports verified some of this progress and, in other instances, called into question the quality of some of the work. For example, while there are notable increases in the percentage of systems with security plans, many Federal systems still do not have contingency plans in place to ensure continuity of operations.

IG reports also continue to identify a number of troubling governmentwide issues and trends such as reoccurring IT security weaknesses, some of which are repeating material weaknesses. Far too many systems continue to operate with serious weaknesses.

Another area highlighted in OMB's report was the need for improved accountability within agencies. The law is very clear on this issue. The agency head is ultimately responsible for the security of their information and systems and is charged with ensuring agency senior officials and the agency CIO fulfill their specific IT security responsibilities.

Agency senior officials are responsible for providing security for the information and the systems which support their operation and assets. In fact, the majority of IT spending within agencies is not on IT infrastructure and networks, traditionally owned and oper-

ated by the CIOs, but rather on mission IT investments. It is within these systems that many weaknesses reoccur.

To address these problems and others, OMB will continue to engage management and leverage the budget processes. While IT security clearly has a technical component, at its core is an essential management function. Most of the Federal Government's IT security weaknesses can be resolved through better management and accountability. Through the budget process, OMB requires agencies to incorporate IT security through the lifecycle of all investments. Failure to appropriately incorporate security puts the investment at considerable risk.

To enforce this requirement, OMB notified those agencies with significant information and system security weaknesses through budget guidance to remediate operational systems with weaknesses prior to spending fiscal year 2004 IT development or modernization and funds. If additional resources are needed to resolve those weaknesses, agencies are to use those fiscal year 2004 IT funds originally sought for new development.

Additionally, OMB continues to enforce IT security through the President's management agenda under the E-Gov scorecard. Agencies may not get to green under E-Gov unless they fully meet specified IT security criteria, including 90 percent of the systems being certified and accredited and that their IG has verified the agency has a plan of action and milestones process in place which meets the OMB criteria. The PMA enables OMB to hold agencies, their senior agency officials and the CIO accountable for IT security performance.

Finally, as we move into the 4th year of these annual IT security requirements, our goal is to improve FISMA reporting instructions so that we more clearly capture results and performance measures continue to mature to focus on key IT security areas. NIST is actively working on the development of new guidelines required under FISMA which will play a significant role in guiding technical implementation of agency IT security efforts.

In particular, as part of the development of OMB's fiscal year 2004 FISMA guidance, we are focusing on the following 3 years: one, evolving the IT security performance measures to move beyond status reporting to also identify the quality of work done; two, the independent evaluations by the IGs continue to be a source of indispensable information, and further targeting of the IG efforts to assess a development implementation and performance of key IT security processes are invaluable; and, three, providing additional clarity to certain definitions to eliminate interpretation difference within agencies and between agencies and the IGs.

In conclusion, I would like to acknowledge the significant work of the agencies and IGs in conducting the annual review and evaluations. It is this effort which gives OMB and the Congress much greater visibility into the agency IT security status and progress.

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains, and OMB will continue to work with agencies, GAO and Congress to promote appropriate risk-based and cost-effective IT security programs, policies and procedures to adequately secure our operations and assets.

I would be glad to take any questions at this time.
Mr. PUTNAM. Thank you, Miss Evans.
[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES

March 10, 2004

Good afternoon, Mr. Chairman, Ranking Member Clay, and Members of the Committee. Thank you for inviting me to speak about the status of the Federal government's efforts to safeguard our information and systems. My remarks will focus on the findings in OMB's FY 2003 Federal Information Security Management Act (FISMA) report and our strategy to address both reoccurring and new information technology (IT) security challenges.

Earlier this month, OMB issued our third annual report to the Congress on agency compliance with IT security requirements in law and policy. FISMA, like its predecessor the Government Information Security Reform Act (GISRA), continues to be a valuable tool in improving the state of Federal IT security – both the security of systems and promoting the protection of information.

In addition to continuing key provisions from GISRA such as the critical role of Inspectors General (IGs) in conducting independent evaluations as well as an increased focus on accountability, FISMA also introduced new provisions. In particular, FISMA directs the National Institute of Standards and Technology (NIST) to develop IT security guidelines in a number of key areas such as the creation of minimum security standards for agency systems. NIST has been actively working with agencies in the development of those standards per their statutory role in providing technical guidelines to Federal agencies.

Background on FISMA Reporting

As you know, FISMA directs Federal agencies to conduct annual IT security reviews and IGs to perform annual independent evaluations of agency programs and systems and report their results to OMB and Congress. OMB's report is therefore based primarily on the FY 2003 IT security reports submitted by agencies and IGs. To ensure consistent reporting across the government, OMB issued FISMA guidance, M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting", which included specific reporting instructions along with quantitative performance measures to more effectively

determine agency status and progress. These instructions for agencies and IGs remained nearly identical to FY 2002 and were mapped directly to the requirements in FISMA. As a result, status against the FY 2001 baseline is easily identifiable.

Other key elements in OMB's FISMA guidance include:

- Continuation of IT security performance measures. Agencies and IGs were charged to report the results of their work against a key set of IT security performance measures. These measures have proved extremely valuable in identifying agency strengths and weaknesses, prioritizing resource decisions, and assisting OMB in our oversight activities.

- Continuation of IT security remediation efforts. OMB guidance continued the requirement Federal agencies to develop plans of action and milestones (POA&Ms) for every program and system where an IT security weakness has been found. POA&Ms must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, identified by the agency, IG, GAO, or OMB, are tracked and corrected. These plans must be developed, implemented, and managed by the agency official who owns the program or system where the weakness was found. An important step for agencies to ensure that have sufficient resources to resolve their weaknesses is tying their system-level POA&Ms directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11). This step is essential to link the justification for IT security funds to the budget process.

- IG assessment of agency POA&M process. To ensure successful remediation of IT security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor remediation efforts. The FISMA reporting instructions requested IGs to assess whether or not an agency has a process in place that meets criteria laid out in OMB guidance.

Additionally, the OMB guidance highlighted new provisions introduced by FISMA:

- Stronger emphasis on configuration management. FISMA requires each agency to develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.

- Codifies requirement for ensuring continuity of system operations. FISMA codifies a longstanding policy requirement that each agency's security program (and particularly each system security plan) include the provision for the continuity of operations for information systems that support the operations and assets of the agency. FISMA explicitly includes in this requirement, information and information systems "provided or managed by another agency, contractor, or other source."

- Development and maintenance of an inventory of major information systems. FISMA amends the Paperwork Reduction Act regarding the major information systems (including major national security systems) operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of "major information system" is found in OMB Circular A-130.

  The FISMA amendments requires that the identification of information systems in this inventory include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. OMB's guidance directed agencies to leverage their enterprise architecture work to create this inventory.

Key Findings from FISMA Report

The OMB FISMA report identifies progress and IT security weaknesses in FY 2003. Agency status against government-wide IT security goals as well as key IT security performance measures in FISMA guidance is provided below.

Progress Against Government-wide IT Security Milestones

OMB established three government-wide goals in the President's FY 2004 Budget and recently provided an update against these measures in the President's FY 2005 Budget.

- **Goal 1** – By the end of calendar year 2003, all Federal agencies will have created a central remediation process to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected. Each agency IG will verify whether or not the agency has a process in place that meets criteria laid out in OMB guidance.
  Status – While each Federal agency does have an IT security remediation process, the maturity of those processes vary greatly. Out of the twenty-four CFO Act agencies, twelve agencies have a remediation process verified by their IG as meeting the necessary criteria. OMB will continue to work with the remaining Federal agencies to achieve the full goal in 2004. OMB emphasizes the importance of an IG verified process by including it as one of three criteria necessary for agencies to "get to green" for IT security on the Expanding E-Government Scorecard of the President's Management Agenda.

- **Goal 2** – By the end of calendar year 2003, 80 percent of Federal IT systems shall be certified and accredited.
  Status – At the end of 2002, 48% of Federal IT systems had been certified and accredited. This percentage increased to 62% at the end of 2003.

- **Goal 3** – By the end of calendar year 2003, 80 percent of the Federal government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment. While agencies have made improvements in integrating security into new IT investments, significant problems remain, particularly in ensuring security of existing systems.
  Status – At the end of 2002, over 60% of Federal IT systems planned and budgeted for IT security requirements as part of the overall development or maintenance of systems. This percentage increased to 78% at the end of 2003.

Agency Progress Against Key IT Security Performance Measures

As discussed, agencies were directed to report their performance against a key set of IT security performance measures. These measures reveal both areas of progress as well as weaknesses. The table below provides the government-wide status from FY 2001 through FY 2003 against a subset of these measures. The data in this table is based on information reported in agencies' FY 2002 and FY 2003 FISMA reports and represents a starting point to get a clearer picture of agency efforts. However, it is important to note that some IG reports called into question the quality of some of this work. Additionally, as some agencies do not have a robust enterprise architecture they may not have an accurate inventory of all of their systems. When reviewing this information, it is also important to recognize that the total number of agency systems tends to change from FY 2001 to FY 2003. A goal of the FY 2004 OMB FISMA guidance is to standardize more of the annual reporting, including clearer definitions to eliminate interpretation differences.

Government-wide IT Security Performance from FY 2001 to FY 2003

Agency	Total No. and % of Systems			No. and % of systems authorized for processing following certification and accreditation			No. and % of systems with security control costs integrated into the life cycle of the system			No. and % of systems for which security controls have been tested and evaluated in the last year			No. and % of systems with a contingency plan			No. and % of systems for which contingency plans have been tested		
	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03
TOTAL	7360	7906	7998	1953	3772	4969	3001	4914	6182	2447	4743	5143	2216	4334	5450	1228	2768	3839
TOTAL				27%	48%	62%	41%	62%	77%	33%	60%	64%	30%	55%	68%	17%	35%	48%

Federal agencies, OMB, the Congress, and GAO are able to track and monitor agency efforts using those measures. While the Federal government is heading in the right direction additional efforts are still warranted. For example, there are notable increases in the percentage of systems with security plans and the percentage of systems certified and accredited. However, many Federal systems do not have appropriate contingency plans in place to ensure continuity of operations. Another continuing area of concern is the low government-wide percentage of systems with tested contingency plans.

Increased Accountability is Critical to Improving IT Security

Even with the strong focus of both GISRA and FISMA on the responsibilities of agency officials regarding IT security, there continues to be a lack of understanding and therefore accountability for IT security performance within the Federal government. The law is very clear on this issue. The agency head is ultimately responsible for the security of their information and systems and is charged with ensuring that agency senior officials and the agency CIO fulfills their specific IT security responsibilities. Specifically, agency senior officials are responsible for providing security for the information and systems that support their operations and assets. They must ensure that the risk to their information and systems is assessed, appropriate controls to protect against the risk are identified, implemented, and tested, and IT security requirements are budgeted. The agency CIO is responsible for the agency-wide information security program, developing and maintaining IT security policies and procedures, IT security training, and assisting agency senior officials with their responsibilities as well as ensuring the security of the information and systems under the CIO's control.

However, agency and IG reports continue to identify a number of troubling government-wide issues and trends, such as:

- Agency and IG reports continue to identify the same IT security weaknesses year after year, some of which are seen as repeating material weaknesses.
- Additionally, while the Federal government appears to be doing a much better job at planning for the security of new IT investments, too many legacy systems continue to operate with serious weaknesses.
- As a result, there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development.

While there are a number of options available to address these concerns they must ultimately be addressed through improved accountability. Even though awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. Ensuring the security of most agency information and systems is not the sole responsibility of the agency CIO. The majority of IT spending within agencies is not on IT infrastructure and networks, traditionally owned and operated by CIOs, but rather on mission IT investments. In fact, historically, over 65% of the Federal government's IT investments are normally mission-IT related. It is within these systems that many weaknesses recur.

IT security is a shared responsibility and holding just one official accountable potentially weakens an agency's ability to properly safeguard its entire collection of IT investments. Through the President's Management Agenda, OMB has increased accountability for agency security performance; however, greater consistency within agencies is necessary.

Plan of Action to Improve Performance

While IT security clearly has a technical component, it is at its core an essential management function. Most of the Federal government's IT security weaknesses can be resolved through better management and accountability. Specifically, OMB will pursue the steps outlined below as a plan of action to both assist agencies in their IT security efforts, promote implementation of law and policy, as well as track status and progress.

Prioritizing IT Funding to Remediate IT Security Weaknesses

Long-standing OMB policy requires agencies to incorporate IT security in the development of both new and existing IT investments and demonstrate that action in their IT budget materials. Agencies must: 1) report security costs for their IT investments; 2) document in their business cases that adequate security controls have been incorporated into the life cycle planning of each IT investment; 3) reflect the agency's security priorities as reported in their POA&Ms; and 4) tie their POA&Ms for an IT investment directly to the business case for that investment.

Failure to appropriately incorporate security in new and existing IT investment puts the investment at considerable risk for funding. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems that have an out-of-date certification and accreditation.

Information from agency and IG IT security reports directly inform the budget process. Specifically:

- Information from agency and IG reports along with their remediation plans identified both agency-wide and system specific IT security weaknesses. Agency POA&Ms provide the corrective actions with estimated costs the agency has determined will resolve those weaknesses.

- Information from IT budget documents, the exhibit 53 and 300, also identify whether appropriate steps to secure both new and legacy IT investments have been undertaken.

This information was particularly useful in prioritizing FY 2004 funding decisions. For example, agencies with significant information and system security weaknesses were directed to remediate operational systems with weaknesses prior to spending FY 2004 IT development or modernization funds. If additional resources are needed to resolve those weaknesses, agencies are to use those FY 2004 IT funds originally sought for new development.

Finally, while funding for IT security has increased from $2.7 billion in FY 2002 to $4.2 billion in FY 2003, historically, a review of IT security spending and security results has demonstrated that spending is not a statistically significant factor in determining agency security performance. Rather, the key remains to effectively

incorporate IT security in agency management actions and implement IT security throughout the lifecycle of a system.

Oversight of Agency IT Security through the President's Management Agenda Scorecard

The President's Management Agenda Scorecard is an important mechanism for both acknowledging agency IT security progress and highlighting significant problems. OMB uses agency IT security materials to help inform the quarterly assessment of IT security under the E-Government scorecard.

To "get to green" under the Expanding E-Government Scorecard for IT security, agencies must meet the following three criteria: 1) demonstrate consistent progress in remediating IT security weaknesses; 2) attain certification and accreditations for 90% of their operational IT systems; and 3) have their IG assess and verify their POA&M process.

In addition to receiving an annual report on agency performance against key IT security performance measures, beginning in December 2003, agencies started reporting each quarter on their status against a subset of those measures. These updates are sent to OMB along with agencies quarterly updates on their POA&M efforts and are also used to inform the quarterly assessment of the President's Management Agenda Scorecard. The PMA enables OMB to hold agencies, their senior agency officials, and CIO accountable for IT security performance.

FY 2004 OMB FISMA Guidance and Upcoming NIST Guidelines

As we progress into the fourth year of these annual IT security requirements, our goal is to move even more toward performance measurement. The ability to clearly determine outcomes and results is essential. Therefore, it is important that FISMA reporting instructions mature to focus on key IT security areas and collect the most useful information to inform agencies, OMB, and the Congress on the status of agency efforts to secure their systems and protect their information. Additionally, NIST is actively working on the development of new guidelines required under FISMA which will play a significant role in guiding technical implementation of agency IT security efforts.

As part of the development of OMB's FY 2004 FISMA guidance, we are focusing on the following three areas: 1) evolving the IT security performance measures to move beyond status reporting to also identify the quality of the work done. For example, being able to determine both the number of systems certified and accredited as well as the quality of the certification and accreditation conducted; 2) the independent evaluations by the IGs continue to be a source of indispensable information and further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes are invaluable; and 3) providing additional clarity to certain definitions to eliminate interpretation differences within agencies and between agencies and IGs.

Measuring the effectiveness of processes and procedures is key. OMB is a strong advocate for documented and repeatable processes for security. We and other experts find certification and accreditation an especially important process because it includes all of the important elements for securing systems. These include identifying risk, effectively planning to manage risk, testing security controls to ensure they are working as intended, understanding interconnections, and planning for inevitable system disruptions and other contingencies. Moreover, a uniform certification and accreditation process across the agencies permits a greater understanding of implemented security controls among interconnected partners.

At the same time, we are equally concerned that merely measuring whether certification and accreditation has been performed, does not tell us the quality of such or whether security is actually improved. If certification and accreditation is truly important, and we think it is, we must not permit it to devolve to the paper chase of past security planning efforts.

Moving to more qualitative performance measures has been our goal since we established a government-wide security baseline. Therefore for the FY 2004 FISMA report, we will ask agencies to report the extent to which any serious security incidents (e.g., root compromises or widespread viruses and worms) occurred on certified and accredited systems and if so to identify the causes. This empirical data will permit the agencies, OMB, and Congress to identify specific areas for improvement.

This data will also permit us to establish a new qualitative performance baseline against which we can measure the future effectiveness of recent and planned NIST guidance required by FISMA.

Conclusion

I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. It is this effort that gives OMB and the Congress much greater visibility into agency IT security status and progress.

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains to improve the security of the information and systems that support the Federal government's missions. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.

Mr. PUTNAM. Our third witness is Benjamin Wu.

Ben Wu was sworn in as Deputy Under Secretary for Technology at the U.S. Department of Commerce in November 2001. In this capacity, he supervises policy development, direction and management at the Technology Administration, a bureau of over 4,000 employees that includes the National Institute of Standards and Technology.

Prior to joining Commerce, Mr. Wu held senior staff positions in the U.S. Congress where he led on issues affecting the U.S. technology and competitiveness policy.

You are, I believe, an alumni of this subcommittee.

Mr. WU. Yes, sir. I did work very closely with the subcommittee and the Committee on Government Reform, but I actually was an employee of the Committee on Science.

Mr. PUTNAM. He worked in Congress from 1988, serving as counsel to Congresswoman Connie Morella and on the Science Committee.

Welcome back.

STATEMENT OF BENJAMIN WU, DEPUTY UNDER SECRETARY FOR TECHNOLOGY, DEPARTMENT OF COMMERCE

Mr. WU. Thank you, Mr. Chairman. It is a pleasure to be back. I thank you for the opportunity to appear before you today again.

As you mentioned, when I worked in the House I also was a lead committee staff on the House Y2K Task Force, and in that vain we had an opportunity to work very closely with GAO and also former Congressman Steve Horn as he developed grades for assessing the agencies' involvement and participation in Y2K activities. It has since evolved into computer security, and I congratulate you for your efforts in continuing that leadership that is so needed on cyber security. Back then, we partnered with GAO.

As you talk about this partnership in progress to move forward on cybersecurity, GAO again is proving to be an excellent partner; and, also, under Karen's guidance, OMB is as well. We see NIST also playing a very important partnership role in that partnership for progress.

I want to thank you for the opportunity to testify about the NIST contributions that strengthen our information security in the Federal Government. I want to focus my remarks on the NIST efforts to implement our assignments under FISMA and some of the challenges that we are facing and confronting.

FISMA's enactment reinforced our longstanding statutory responsibilities for security research and for developing Federal information standards and guidelines. With FISMA, Congress gave NIST a vote of confidence about its abilities to work and further this research, and we do appreciate that recognition.

NIST standards and guidelines form the basis of the Federal Government's ability to improve cybersecurity. Our security work at NIST is being done out of our Information Technology Laboratory, which develops tests, metrics, as well as guidance for building trust and confidence in IT systems that are now so pervasive in our Nation's economy.

Behind me is Susan Zevin, who is the leader of our Information Technology Laboratory, and also Ed Roback, who is the head of the

Computer Security Division at NIST. Those two and their team at NIST helped build a trust of users of IT systems by concentrating on techniques and tools to manage, to use and improve IT security system. NIST's success really relies on its status as an objective third party working with private sector vendors, standards development organizations, and consortia.

Mr. Chairman, I want to give you a status report on where NIST is in terms of its FISMA responsibilities.

The general responsibilities that were assigned to NIST under FISMA included developing IT standards, identifying information security vulnerabilities, assessing private sector policies, assisting the private sector as well, and also evaluating security policies.

FISMA also contained a number of specific assignments to NIST, and they included the development of standards and guidelines, recommended types of information systems, as well as minimum information security requirements, an Incident Handling Guideline, and security performance indicators, as well as an annual reports to the committee.

To summarize the progress that we have made since FISMA became the law in December 17, 2002, significant progress has been made on the specific assignments and many have been completed. They include the FIPS Publication 199, which was completed in January 2004; the NIST Special Publication 800–60, which is to be completed this summer, and a draft is now available; the NIST SP 800–53 is also ready for completion in December 2005, and the public draft is available; the NIST SP 800–55 to be completed in July 2003; the NIST SP 800–59 to be completed in August 2003; and also the NIST SP 800–61, which was just completed this past January.

But, as Bob mentioned, we are concerned because Congress was unable to meet the Presidential budget request for the NIST Cybersecurity Division in the fiscal year 2004 appropriations and, as a consequences, Mr. Chairman, although we continue to give FISMA activities priority in our budgeting process, the guidelines, the standards, and related research in the following areas may not be able to be accommodated within our fiscal year 2004 funding level and have to be scaled back.

They include guidelines on archiving and disposal of information, checklists and guidelines, new security protocols, operating our Computer Security Expert Assist Team, supporting the NIAP, minimum security recommended requirements, as well as some of our implementation for IPv6.

At current levels of funding, we've also had to delay a number of other activities which I will not list in total.

But, let me be clear, due to prioritization within the Computer Security Division, none of the specific tasks that are assigned to us under FISMA are affected. Rather, they're proceeding as scheduled as best we can within the timeframes allowed under legislation. But we feel that NIST is so uniquely poised to do so much more, and we are limited really only by our budget constraints.

Before Congress now is the President's fiscal year 2005 budget request that includes a proposed increase of $6 million for NIST to address the key national needs in cybersecurity. With the proposed increase of $6 million for 2005 with the current level funding——

Mr. PUTNAM. Did you say million or billion?

Mr. WU. Million. We would love for it to be billion, but we also understand the constraints on the Federal budget.

But coupled with the current $10 million that NIST has for its efforts, we believe that NIST can work more effectively with industry and government agencies to accelerate solutions to critical cybersecurity issues.

Additionally, this would include costs that would allow us to work together with the Homeland Security Department's Science and Technology Directorate, as well as the Information, Analysis and Infrastructure Protection Directorate in the National Cyber Security Division.

We also would like to see if we can continue to provide other agency reimbursable work and partner with other Federal agencies so that we can have people tap into the NIST expertise and also allow for other agencies to meet their FISMA responsibilities.

In conclusion, Mr. Chairman, the standards and guidelines produced by NIST are key to the Federal Government's ability to improve cybersecurity. NIST's impact reaches far beyond just the Federal system, since the NIST guidelines are also used by State and local governments as well as often adopted by the private sector, domestically as well as internationally.

NIST takes its cybersecurity role very seriously and will work with the committee to ensure that we are able to carry out our mandate to work with industry, with academia and standard development organizations to ensure the secure flow of vital and sensitive information throughout our society. We applaud the committee for its leadership and also for detailing a specific leadership role for NIST to play in supporting that effort.

In the FISMA activities those already accomplished as well as those currently under way will lead to a more consistent risk-based and cost-effective IT security at all Federal agencies. We look forward to working very closely with you, OMB as well as GAO.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Wu follows:]

Statement of

Ben Wu
Deputy Under Secretary
Technology Administration

U.S. Department of Commerce

Before the
Committee on Government Reform
Subcommittee on
Technology, Information Policy, Intergovernmental Relations
and the Census
U.S. House of Representatives

"Information Security in the Federal Government: One Year into the Federal Information Security Management Act"

March 16, 2004

Thank you for this opportunity to testify today about the contributions of the National Institute of Standards and Technology (NIST) to strengthen information security in the Federal government. I would like to principally focus my remarks on our important efforts to implement the assignments to NIST in the Federal Information Security Management Act (FISMA) of 2002 and some of the challenges we confront.

The Context of NIST Information Security Work

FISMA reinforced our long-standing statutory responsibilities for conducting security research and developing Federal information standards and guidelines. We thank the Congress for this "vote of confidence" in our past work, with an expectation of continuing successful achievements in the future.

Information security is one of the most critical issues facing industry and government. The technological and scientific base that makes this country so strong is continually improving its ability to compete globally through tremendous advances in the capabilities of IT systems. As a nation, we are challenged to keep up with the growing complexity of our new technologies and the increasing sophistication of those seeking to maliciously interfere. Those "bad guys" continue to find new ways to breach our systems. While we focus on current implementations, new technology developments in IT systems and in other disciplines that increasingly rely on IT systems are coming on-line at an accelerating pace.

NIST standards and guidelines form the basis of the Federal government's ability to improve cyber security. Our information security work at NIST is conducted in our Information Technology Laboratory (ITL), which develops tests, metrics, and guidance for building trust and confidence in the IT systems that are now pervasive in the nation's economy, its organizational, governmental, scientific and technological infrastructure. NIST builds the trust of users of IT systems by concentrating on techniques and tools to manage, use, and improve IT systems, from single-user desktops, to highly complex multi-server, multi-node, wired and wireless systems that manage trillions of dollars in daily financial transfers, control power generation and distribution, and generate scientific and technological innovation.

NIST's success relies on its status as an objective, neutral, third party, allowing it to leverage its unique competencies to develop consensus solutions among private sector vendors, standards development organizations, and consortia. Unique competencies in smart cards, biometric devices and biometric analysis are applied to address the needs for better identity, authentication, and credentialing and to thwart identity theft. Tools, tests and metrics in software quality allow developers to "harden" code against "buggy" software and to protect against creation of unintended vulnerabilities; models, protocols and specifications for advanced networking technologies add resilience against catastrophic failure and provide agility to create networks where infrastructure is destroyed or does not exist. Our unique capabilities in theoretical mathematics,

computational science and statistics enable other scientific disciplines to utilize IT systems to explore and innovate at the edge of technological frontiers.

NIST continues to take strides toward securing the nation's systems and information through development of tools, tests, metrics, and guidance but much remains to be done. FISMA and the Cyber Security Research and Development Act (CSRDA) of 2002 provide a roadmap for NIST to follow in performing this critical role. Today, I will discuss NIST's role in information security in the Federal government, one year into the Federal Information Security Management Act. Specifically, I will address:

- NIST responsibilities under FISMA;
- Summary of Standards Required by FISMA;
- Impact of Budget Restraints on NIST's Responsibilities under FISMA;
- Resources necessary for NIST to fulfill responsibility under FISMA;
- Other Supporting FISMA-related Activities at NIST; and
- Beyond our Current Plans and the FY 2005 Initiative.

NIST Responsibilities under the Federal Information Security Management Act of 2002

General responsibilities assigned to NIST under FISMA include:

- Developing IT standards for Federal systems, specifically to include security standards and guidelines;
- Conducting research to identify information security vulnerabilities and developing techniques to provide cost-effective security;
- Assessing private-sector policies, practices, and commercially available technologies;
- Assisting the private sector, upon request; and
- Evaluating security policies and practices developed for national security systems to assess potential application for non-national security systems.

FISMA also contained a number of specific assignments to NIST, including development of:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category;
- Minimum information security requirements, such as management, operational, and technical security controls, for information and information systems in each such category;
- An Incident Handling Guideline and a Guideline to Identifying a System as a National Security System;
- Security performance indicators; and
- An annual public report.

Summary of Standards Required by FISMA

I would like to summarize the progress that we've made since FISMA became law on December 17, 2002. Significant progress has been made on these specific assignments and many have been completed.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (completed January 2004)

FISMA directed NIST to develop an information categorization standard for the Federal sector to support inter-agency, intra-agency and third party information sharing and ensure that consistent sensitivity (or impact) designations were applied. This is a crucial first step in the overall risk management process in that these categorizations influence an organization's determination regarding what security controls should be applied to protect the confidentiality, integrity and availability of the information. A problem, which had been noted by OMB, was the inconsistent application of security controls as information was shared across agency and third party boundaries. FIPS 199 provides a standard framework for government-wide use in information designation.

NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (public draft now available; on track for completion in Summer 2004)

The companion guidance for FIPS 199, this Special Publication recommends a process by which agencies may categorize their systems and a methodology for effectively applying the principles included in FIPS 199. It presents common categories of information used by agencies and suggests default sensitivity or impact levels for these common information types (financial, personnel, health, etc.). It also provides a discussion and rationale for the generally recommended categorization for each information type, while recognizing that variances from the proposed default may sometimes be appropriate. Because of the numerous system interconnections and extensive use of data aggregation today, this guide helps highlight for agencies how the initial categorization can be influenced by special factors (factors such as mission and direct impact on mission). Again, it presents a common base of rationale which can be used government-wide to derive the impact of the loss of confidentiality, integrity and availability. This will assist in minimizing disparate treatment of information as it crosses organizational boundaries and a more cost-effective and consistent application of security resources.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (public draft available; on track for completion of FIPS 200 by December 2005)

This guidance document (which will form the basis for a future Federal standard, FIPS 200) defines security control baselines or minimum standards based on the impact category (Low, Moderate and High) of the information system as determined by the

agency, using FIPS 199 and NIST SP 800-60. It also provides guidance for tailoring the baseline controls based on risk and cost-benefit assessments.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems* (completed July 2003)

This guideline, developed under FISMA and at the specific request of OMB, provides over twenty specific metrics that can be used by agencies to develop performance indicators for their programs. This guideline is now being used by agencies in developing their reporting under FISMA.

NIST SP 800-59, *Guide for Identifying an Information System as a National Security System* (completed August 2003)

This guidance was developed in conjunction with the Department of Defense and provides agencies criteria for identifying an information system as a national security system.

NIST SP 800-61, *Computer Security Incident Handling Guide* (completed January 2004)

NIST Special Publication 800-61, Computer Security Incident Handling Guide, assists organizations in mitigating the potential business impact of information security incidents by providing practical guidance on responding to a variety of incidents effectively and efficiently. Specifically, this document discusses the following items: 1) establishing a computer security incident response capability, including policy, procedure, and guideline creation; 2) selecting appropriate staff and building and maintaining their skills; 3) emphasizing the importance of incident detection and analysis throughout the organization; 4) maintaining situational awareness during large-scale incidents; and 5) handling incidents from initial preparation through the post-incident lessons learned phase, including specific advice on five common categories of incidents.

Other NIST Guidelines Currently in Development in Support of FISMA include:

- **NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems*** (under development, draft expected in Summer, 2004, delayed due to budget cuts)
- **NIST SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*** (public draft now available; final draft expected Summer 2004)
- **NIST SP 800-63, *Recommendation for Electronic Authentication*** (public draft Jan 2003)
- **NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*** (Oct 2003)

- **NIST SP 800-50,** ***Building an Information Technology Security Awareness and Training Program*** (October 2003)
- **NIST SP 800-65,** ***Integrating Security into the Capital Planning and Investment Control Process*** (public draft expected by July 2004)
- ***Guideline on Voice over Internet Protocol Security*** (public draft Fall 2004)
- ***Guideline on Implementing IPSec*** (public draft Fall 2004)
- ***Guideline on use of IEEE 802.11i*** (secure wireless), (public draft Fall 2004)
- ***Guideline on Personal Digital Assistant Forensics*** (public draft Fall 2004)

Budgeting for NIST's Responsibilities under FISMA

Although we continue to give FISMA activities priority in our budgeting process, guidelines, standards, and related research in the following areas can not be accommodated within our FY 2004 funding level and have been scaled back or delayed:

- Guideline on archiving and disposal of information technology systems;
- Checklists and guidelines for effective implementation of COTS products (explicitly mandated by CSRDA);
- New security protocols for the core Internet, leaving a critical set of vulnerabilities that cannot be secured;
- Operating our Computer Security Expert Assist Team;
- Support to the National Information Assurance Partnership (reduced);
- Minimum-security recommended requirements for the most basic computer systems used by small businesses and home users;
- New investments in network security for wireless devices; and
- Implementation and use of IPv6.

At the current level of funding, we have delayed the following items previously included in our plans for FY 2005:

- Implementation guideline on use of minimum requirements for Federal systems (800-53)
- Comprehensive guideline on FISMA and other security requirements in the System Development Lifecycle
- Security program manager's guideline to information security program management
- Guideline on use of card-based technologies for cybersecurity
- Executive Guide to Cybersecurity
- Security requirements for operating systems, firewalls, biometrics, and process control systems
- Guideline for testing of operating systems, firewalls, and biometrics against the requirements
- Guideline for retrofit of cryptographic security modules for SCADA

- Guideline of conformance testing methods for security in process control systems
- Comprehensive Standards for Random and Pseudo-Random Number Generation to support strong cryptographic keys and strong algorithm initialization vectors
- Wireless Key Management for Secure Communications
- Incremental specifications for automated architectural security development
- Cybersecurity architectural guideline
- Standard set of Applications Programming Interface (APIs) for the specification, composition, enabling and disabling of policies that are amenable to uniform testing and could be applied to emerging technologies

Due to prioritization within the Computer Security Division, none of the specific tasks for developing guidelines under FISMA are affected; rather they are proceeding on schedule per the timeframes outlined in the Act.

Resources necessary for NIST to fulfill responsibility under FISMA

Now before the Congress is the President's FY 2005 budget request that includes a proposed increase of $6 million for NIST to address key national needs in cyber security. With the proposed increase of $6 million to NIST's current funding level of approximately $10.0 million, NIST will be able to more effectively work with industry and government agencies to accelerate solutions to critical cyber security issues. This specifically includes working with the Department of Homeland Security through its Science and Technology Directorate, as well as the Information Analysis and Infrastructure Protection Directorate's National Cyber Security Division to enhance collaborative efforts begun in 2003. This proposed expansion of NIST's current program will allow for additional deliverables in FY 2005 and a critical start to long-term work in key areas including:

Enhancing security, critical infrastructure application, and communication protocols. Numerous protocols are being developed for special purpose security, critical infrastructure and communications. The number of formal and *ad hoc* protocol standards precludes the ability for security specialists to participate in each effort; however, drawing upon the security, protocol, critical infrastructure, and vendor community, security guidance could be developed to provide protocol designers with advice and input into the design of secure protocols, hence enhancing security, critical infrastructure application, and communication protocols. Automated web-based testing for implementers of widely used protocols with security consequences could also be developed and provided to help assure correct implementation.

Expand the NIST Cryptographic Toolkit to include limited power, small-sized computing environments. Secure standard cryptographic mechanisms tailored for use in embedded devices are not being developed. Without such standards, security in these new technologies such as those associated with personal data assistants and blackberries already is inadequate as designers adapt existing standards to "fit" the low

processing power and bandwidth available on an *ad hoc* insecure basis. As vulnerabilities are discovered, expensive patches must be applied and, since patching never achieves the desired coverage, system security exposures remain. The answer is to build products correctly from the start, but the available time window for action is closing. The NIST cryptographic toolkit will eventually be expanded to accommodate these limited power, small-sized computing environments. Guidance will also be developed and promulgated on where the new standards are applicable. The next generation of agile cryptographic security standards for process control, embedded systems, and mobile applications also will be developed. The key for effective use of these guidelines and standards throughout the community of developers is the timing of their release.

Fix broken wireless security standards by identifying, prioritizing, and accelerating approaches to securing wireless devices. Fixing insecure wireless security standards by identifying, prioritizing, and accelerating approaches to securing wireless communication protocols will speed the improvement of wireless security standards and ensure that insecure "interim fixes" do not become entrenched. NIST will participate in standards bodies activities to provide security expertise. Proof-of-concept prototype(s) for new wireless security technologies will be developed by leveraging, to the extent practicable, existing solutions (e.g., Public Key Infrastructure (PKI), Certificate Management, etc.). Guidance on wireless security design, implementation, and administration best practices will be written. Approaches to wireless security policy expression and enforcement, mobile device user authentication, secure ad hoc networking protocols, and intrusion detection in ad hoc networks will be developed. This is a one-time critical opportunity to make significant security enhancements, and speed is essential.

Metrics to understand, express, and improve our ability to build secure networks and systems from individually understood components. Systems of growing complexity tend to emphasize the challenge of building secure systems from secure components. There is a need to develop metrics to understand, express, and improve our ability to build secure networks and systems from individually understood components. Taxonomies could be developed for security metrics associated with assembling a networked computer system from components while ensuring it maintains desired security properties. Additionally, advanced methods could be developed to express security requirements for integrated systems, and metrics to enable rapid testing. Metrics to facilitate integration of components with known security exposures and risks are needed. Formal modeling of security properties in an architecture will be investigated. This is a major, long-term research effort, which could be launched in FY 2005 with appropriate funding.

Advanced means to cost-effectively control access of individuals and automated services to information and other automated services. Today's cyber and physical threats along with legislation such as the USA PATRIOT Act, HIPAA and various national and foreign privacy laws have stressed the need to develop advanced means to cost-effectively control access of individuals and automated services to information and

other automated services. This includes advanced access control meta models that will be capable of flexible, cost-effective implementation of strong cybersecurity access policies and standardized access policy definition frameworks (e.g., XML-based vocabularies). These frameworks could then be mapped to different enforcement mechanisms to develop a scalable, interoperable, enterprise-wide authorization-management framework.

Test procedures and guidelines for retrofitted cryptographic modules for system control and data acquisition (SCADA) systems. While last summer's black-out along the East Coast was attributed to an unfortunately and unlikely train of natural events, it was a bold reminder of the delicate state of some portions of our critical infrastructure and the need for significant upgrades to the IT supporting it. The security of SCADA and building control systems could be enhanced. With requested funding for FY 2005, test procedures and guidelines for retrofitted cryptographic modules for SCADA systems will be developed and standards for SCADA and other industrial control system security will be validated. Performance and conformance test methods for process controls, protection profiles for process control systems, and protocol standards for more secure communications for integrated building systems and services controls will be developed under this program.

Guide on approved media sanitization and disposal techniques. Approximately 5 billion gigabytes of information was created in 2002, equivalent to half a million libraries the size of the Library of Congress, or about 800 megabytes per person per year. There is a critical need for a guide on approved media sanitization and disposal techniques, which address today's new technologies such as mobile devices (Blackberry, PDAs), removable media (compact flash, secure digital), and hybrid devices (PDA/cellphones). As you may imagine, with the volume of digital information being produced and its rate of growth we receive numerous requests for appropriate disposal techniques. With requested funding increases, guidance in this area could be ready for public comment in FY 2005.

Other Supporting FISMA-related Activities at NIST

Cryptographic Modules for Federal Government Use. The Cryptographic Module Validation Program, operated in conjunction with the Government of Canada's Communication Security Establishment, has now validated over 750 modules. Our statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without our program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography. Federal agencies are required to use validated modules in cryptographic applications. We expect that 200 or more modules will be submitted for validation within the next year. We continue to expect this program to grow, to include additional laboratory accreditations. Requested increases will enable us to enhance and expand this program.

Consensus-based recommended security requirements and corresponding testing procedures. In recent years we have worked with industry to develop the "Common Criteria" which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership (NIAP). There is a critical and continuing need to develop consensus based recommended security requirements and corresponding testing procedures for commonly used security and security-related technologies such as operating systems, routers, and intrusion detection and prevention systems. The FY 2005 budget increase would provide for the development of the most critical security requirements. These requirements and procedures increase the security of IT products, bring consistency to the testing process, reduce the need for government oversight during evaluations, ultimately decrease the cost to industry for the validation of products and provides more evaluated security products to both Federal users and the public in general.

National Information Assurance Partnership. You may be aware that the National Strategy to Secure Cyberspace calls for a review of the NIAP. We have had staff discussions with NSA, the NIAP laboratories, and vendors to identify ways we might improve the process, through research, process changes, and to understand the resources needed for NIAP to fully succeed. Additionally, we are participating on the industry common criteria/NIAP task force, established at the December 2003 Department of Homeland Security National Cybersecurity Summit. The output of that task force, which NIST co-chairs, is expected to issue its report shortly and may interest this Committee. Requested increases are needed for the development of additional security requirements and corresponding testing procedures, and to more generally improve NIAP processes based on recommendations that come out of the NIAP review process.

Beyond our Current Plans and the FY 2005 Initiative

In recognition of the constrained budget realities, we have focused on the most critical items in our current program plan and the proposed FY 2005 budget. However, in addition to the funding we receive from Congress each year, we do conduct reimbursable work for other agencies. I thought it would be helpful to the Committee to share some of the information security services that NIST could offer to other agency sponsors.

National network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines. By December 2005, NIST's *Recommended Security Controls for Federal Information Systems* will by law become *Minimum Security Controls for Federal Information Systems*. This will form the basis for a risk-based certification and accreditation of Federal information systems, giving agency report cards new meaning. Work must be completed to create a national network of accredited organizations capable of providing

cost effective, quality security assessment services based on the NIST standards and guidelines. This will build more assurance in existing processes, build a higher degree of consistency into certification processes and provide for a more cost-effective approach to certification for which the resources expended for certification track with the sensitivity of the particular system.

Guideline on the effective integration of security into the Federal Enterprise Architecture. Another area of major importance is the development of detailed guidance on the effective integration of security into the Federal Enterprise Architecture (FEA). Although the FEA framework is in place, an instructive guide assisting agencies in correctly mapping current security standards and guidelines to layers of the existing architecture is needed to ensure that the Enterprise Architectures developed by agencies reflect and accommodate security components. The Federal CIO Council has begun work in this area and NIST will continue to partner with the Council on this effort.

Comprehensive security checklists and benchmarks. Both hardware and software are typically shipped already configured for ultimate functionality and interoperability and not for secure use. NIST could greatly assist the public *and* private sector by delivering a series of guidance and supporting templates for decision-making on system settings and configurations. Security checklists and benchmarks, i.e., recommended security settings for specific commercial products such as firewalls, operating systems, and database systems, could help organizations and individuals to help themselves while still taking full advantage of emerging technologies and still reduce threats such as identity theft, denial-of-service or other malicious attacks on information systems. DHS has graciously been supporting some important NIST work in this regard and we will be able to maintain a web-based portal and solicit checklists, and perhaps internally produce one or two checklists in FY 2005 and each year thereafter. To be comprehensive, checklists should exist for *all IT products with security functionality widely used in the Federal government*, as is required under CSRDA.

Guidelines for users and system administrators to reduce spam. The reduction of spam has become a high priority from offices to households across the country. NIST recently completed a SPAM workshop on the current technologies and approaches to minimizing the costs and related impacts of SPAM. Research in support of spam filtering and guidance for users and system administrators to reduce spam could greatly assist agencies in minimizing this ongoing problem. Perhaps more importantly, with the growth of voice over IP, spammer techniques will be employable against two of an organization's access points to the outside world. Therefore work should also be done to understand new security vulnerabilities introduced by spammer techniques used in conjunction with this emerging technology and the viability of countermeasures.

Quality Code and Today's On-going Virus and Vulnerability Wars. You are probably familiar with the on-going daily virus wars that are currently raging, including viruses propagated by e-mail. In the early 1990s, NIST conducted anti-virus work, which was helpful to the establishment of today's robust anti-virus industry. The anti-

virus industry is to be commended for keeping up with the continuing onslaught of viruses with timely updates to their virus definitions. In addition to viruses, with the continuing discoveries of vulnerabilities in commercial software and need to patch software, we are presently in a never-ending game of catch-up for users to stay up to date with the latest viruses and latest patches provided by vendors. And we are losing that catch-up game.

Of course, this is not a game but a serious security matter. Users do not keep their anti-virus programs up-to-date and do not apply software patches in a timely manner – if at all. When one steps back, it really highlights the need for the development of more secure code – code that will be resistant to viruses and other attacks that exploit vulnerabilities in software and hardware. We know how to build better code, but it is time consuming and tedious. The national annual costs of an inadequate infrastructure for software testing is estimated to range from $22.2 billion to $59.5 billion. We need to develop better secure code building technologies and standards, to include tests that vendors can run during development to produce high quality code and not impact their time-to-market requirements. NIST is ideally positioned to be able to do such work to help industry and thereby reduce the costs and security exposures for agencies and other critical users in the nation.

Closing

The standards and guidelines produced by NIST are key to the Federal government's ability to improve cyber security. NIST's impact reaches far beyond Federal systems. NIST guidelines are frequently used by state and local governments as well as by the private sector. In actively working with voluntary national and international standards development organizations, NIST guidelines and standards in areas such as cryptography and information security management are frequently adopted around the globe.

NIST takes its role in cybersecurity seriously and will work with the Committee to ensure that we are able to carry out our mandate to work with industry, academia, and standards development organizations to assure the secure flow of vital and sensitive information throughout our society. We applaud the Committee for its leadership and defining a critical role for NIST to play in supporting that effort. The FISMA activities – those already accomplished and currently underway – will lead to more consistent, risk-based, and cost-effective IT security at Federal agencies. The opportunities identified above would further strengthen Federal security.

These examples of our work and accomplishments demonstrate NIST's commitment to information security, across the government and the nation. They also demonstrate the base upon which NIST hopes to enhance our efforts, in line with the President's FY2005 budget request. It is an absolutely critical national need.

I am grateful to Chairman Putnam for holding this hearing, and for his support of NIST's critical role under FISMA.

I will be pleased to answer your questions.

Mr. PUTNAM. Ms. Evans, in your 2003 FISMA report you say that ensuring the security of most agency information and systems is not the sole responsibility of the agency CIO. While I can understand where you're coming from, that everybody has a role to play in their own piece of the agency or department, there's an old saying that everyone's responsibility is no one's responsibility. How do you see increasing the awareness of all employees to their information security responsibilities while still having some accountability built into the system.

Ms. EVANS. I believe that there is accountability built into the system. The way that is, is that FISMA's very clear that it holds the agency head responsible for the cybersecurity posture of the agency. That agency head then manages what risk do I want to go forward with, and there is a tiered approach into this where the CIO manages from an enterprise prospective. So based on policies and guidelines that come out from OMB and from Congress, the CIO then manages across the enterprise or through the corporation, so to speak.

But then, as that then goes down, each then program officer—or in this case the way that we refer to this is agency senior officials, because it could be staff office, it could be assistant secretary, is responsible for ensuring their portion of that cybersecurity posture. The agency head determines what risk are they willing to live with and then they move down through the structure to ensure that the accountability is built into that.

So the point of the report is to say that, although the CIO puts together the enterprise solutions, so to speak, and the policies and the procedures, the CIO also then ensures that investments that are occurring within those program offices will meet that risk posture that the Secretary wants to have as a whole.

So we believe it is clear, but we also need to articulate that it is important that everybody has to do their portion of what is responsible here, from the very first employee when they come on board, to being aware that maybe I shouldn't put a disk into my computer that I brought in from home, to the agency head, the Secretary, who has to manage all of the assets.

Mr. PUTNAM. What negative consequences have there been to the agencies who received failing grades or even backslid in their scores and things like that? What action has been taken to demonstrate accountability?

Ms. EVANS. We have been working through a series of processes that we have in place.

First off, there's the President's management agenda scorecard. The E-Gov scorecard manages the progress of the agencies going forward, and cybersecurity is a major portion of that. There is a quarterly grade that we give to each agency which clearly holds again the agency head responsible as well as going down through the agencies because it recognizes within there everyone has to play a part in the cybersecurity piece.

But also, additionally, through the budget process this year we went forward, and cybersecurity is an important issue for this administration, so we gave specific guides to the agencies through the budget process of how we wanted to ensure that they were taking and looking at what they needed to do to secure their assets. So

they were given specific guidance through the budget guidance that said you have to turn in a plan and that this plan is specifically focused on certification and accreditation which really deals with the business process and how you manage cybersecurity across your enterprise.

They were given specific timeframes to turn those plans in to us and the costs associated with making that happen so that we can achieve the goals that we have set out for ourselves which we didn't achieve that we had laid out in the fiscal year 2004 budget.

So we are now in the process of looking at these plans and working with the budget side as well as the management side within OMB and then each of the agencies to make those plans a reality and to ensure that we go forward and we secure those systems.

Mr. PUTNAM. In reading your testimony, you indicate 12 agencies have a remediation process verified by their IGs as meeting the necessary criteria. Do you know the agencies who did not have a remediation process? You are only batting 500.

Ms. EVANS. Yes, I know. That's not a very good grade. I can give you the specific agencies. It's in the report. But——

Mr. PUTNAM. Are they the big boys? That's really what I want to know.

Ms. EVANS. It's a mixture of agencies. But the remediation process is dealing with—that's an IG verified—we have the IG verify that process. That deals with that they have a process in place that ensures that, as they go forward and they purchase new types of things or that a new vulnerability comes up, that they have a process in place that allows them to remediate that weakness. That includes things like configuration management and those type of processes to go forward.

We gave 18 agencies additional guidance through the budget process to deal with certification and accreditation so that gets to the issue of ensuring that they really have identified what their system inventory is and that they are going through and they have a process in place that allows them to certify and accredit these systems which really then gets the discipline in place for you to really evaluate as you go forward.

Mr. PUTNAM. I'm looking back to my opening statement. Only five agencies have completed reliable inventories. That's correct, right?

And we've been doing this for 4 years.

Ms. EVANS. Yes, sir.

Mr. PUTNAM. So you're saying that your budget guidance language tells them what they needed to do to get it right. But did anything actually happen? I mean, if only five have done it, the other 19 are saying, well, we're in pretty good company.

Ms. EVANS. Are you asking what specific actions we have taken since the budget guidance has been issued to the agencies?

Mr. PUTNAM. I guess I'm asking if there's been anything other than guidance.

Ms. EVANS. Oh, sure. As part of that guidance process and as we go forward and as we've outlined previously, there are tools that are available to us at OMB such as apportionment of funds.

The budget guidance is very clear. When a budget guidance goes out and we tell the agencies you cannot spend new development

dollars in this area because they have been categorized as new development dollars, that's just not saying you can't spend it. It's the OMB budget accountants working with us, that there is a process that we have in place with OMB that doesn't allow those dollars to be released to the agencies. So dollars are not moving out until we have these plans and we feel comfortable that the agencies are really looking at this.

To get to your issue about inventory, we really believe that it is tied to the management of the portfolio as well as investments.

You really have to know what you have to be able to come forward with a good business case to say, for example, I have a modernization plan, here is my architecture, here is my as-is architecture, here is the to-be. Through our efforts on the architecture as well as managing the portfolio and the business cases, this will really make the agencies really have a good process in place, and it really will identify the inventory so that we can say there are so many servers, there's so many of these, there's so many of those, this is the cost that it will take to upgrade that, and here's the benefit associated with that.

So we think through the combination of all these management practices it will get to the heart of the issue of what do we own, how are we going to secure it, how are we moving forward with a modernization plan. We believe that the Federal enterprise architecture and the architecture efforts of the agencies really lend to that and really are assisting the agencies to really put that discipline in place.

Mr. PUTNAM. So can you tell me how many dollars and how many specific modernization or development requests have been apportioned pending the successful completion of reliable inventory?

Ms. EVANS. Well, I have gone back, based on the previous hearing; and if you haven't gotten this answer I can give it to you now. There is $9.97 billion associated with office automation, telecommunications and infrastructure. That's total. So that includes development and steady State dollars.

We are working with each agency. I can take that back and find out specifically if we can release that information to you, but we have apportioned agencies. We really would like to work with the agencies in a positive way to be able to move forward and not necessarily single out one agency over the other.

I think it's pretty obvious, based on your scorecard of going through of what agencies we're really working with very closely, as well as agency IG reports and the FISMA report itself. You can see the variance in the system, and you can see how the statistics are, that you know pretty much where the agencies we're working with.

Mr. PUTNAM. It just seems to me that the new dollars for upgrades of systems and purchases of new systems and development would just come to a screeching halt if you really had to be compliant with FISMA before you got anything new.

Ms. EVANS. Well, it would depend on what your plan is, also, going forward. Some of the systems—and if you look at the technologies that are outlined in the GAO report that they're releasing today, some of those do require a certain technology solution there which will require a purchase. But it may not necessarily be the

same purchase that you were intending to do, for example, for a business system upgrade.

You may then say, OK, I am the Assistant Secretary in charge of this particular office. I have a huge program that really has a risk that is being imposed over here on all the rest of the assets within the department, and I'm the one who doesn't have a good plan in place. I have not certified and accredited my systems. I am not the one—you know, I'm the one who is holding the department back.

So then the CIO with their technical staff would talk with that and work with that Assistant Secretary, but they would make those decisions based on the priorities of where they want to be.

So if it's a choice between upgrading a financial management system, and we're saying this is what you have to do, they put a plan in place in order to execute what we're saying you have to do, it's to their advantage to do it in the most cost-effective way. Because if they really need that financial system upgraded, which I'm just using as an example here, then they would do this in an expeditious way so that they could still use those development dollars.

Mr. PUTNAM. Well, I think that you're making progress generally across the board. You've got an 80 percent goal to integrate security and new investments, and you're up to 78 percent. That's pretty good stuff. That's kind of hard to argue with.

But it's also hard to get around the fact that only five agencies know what they own. Everybody's held accountable for their inventory. Even in a little old congressional office, you cannot get rid of a VCR that's 12 years old without taking it off your inventory and all this stuff.

It just seems like it's a very, very basic thing that these agencies ought to be able to get their arms around and then be able to say, well, we have 15 systems or 15 desktops that are unaccounted for and they're, on average, 13 years old. So they probably got thrown out a long time ago. It is probably a safe bet that they are unaccountable because they were thrown out.

If it's a secured computer at the Department of Energy, it might be a different issue. But just knowing what you have seems to me to be the basic criteria before you do any of the other stuff. You can't secure what you don't know you have. You can't certify or accredit what you don't know you have.

It just seems like, above and beyond the scorecard and the grades and the F's and the A's and all that, the fact that only five agencies really know what they own is very troubling.

Ms. EVANS. I would say that I agree with you, sir, and that we're going to continue to work with the agencies. We believe that some of the programs that we've moved forward on, things such as Smart Buy and those types of initiatives, through several of these processes will get the agencies really focused on asset management, software management, inventory control, those types of things.

Technology continues to evolve; and many times if we make it very onerous that work can't get done, people have a tendency to bypass that security as well. There's a lot of technologies out there that make use of wireless technologies that they can put their own network in case—because the CIO becomes so oppressive that they cannot get their work done. So it is a balance of being able to go

forward and have good security but also, as you said, to have good inventory control and have good business processes in place so that we're totally accountable for our dollars.

Mr. PUTNAM. You said in your testimony as well that it is important that FISMA reporting instructions mature. What do you mean by that?

Ms. EVANS. Well, pretty much you've hit the issue on the head. It is that we're going through the process right now where we have metrics, where the agencies are self-recording. So when we say we have a goal of 80 percent of the systems being certified and accredited and then we have a percentage of 62 percent of those systems being certified and accredited, it's really what is the validity of that number. Because the basic premise of the inventory is faulted. But we also believe that, because of the reporting that we have and the oversight and this is 3 years going into the 4th year, that we can now, because the baseline is there, really start dealing with more mature aspects like the quality of certification and accreditation. What can we do to help the agencies to get good inventory control and process so that we can then say, what is a system, and have a clearer definition of what is a system so that when I put an inventory control process in place I can give you a clear answer and then you can compare for sure agency to agency, system to system, inventory to inventory.

Mr. PUTNAM. So you don't necessarily recommend legislative changes to the FISMA reporting requirements?

Ms. EVANS. I would say at this particular point based on what we have, no, sir.

Mr. PUTNAM. You also say that the independent evaluations by the IGs are indispensable, and I would agree with that.

What do we do about the IGs who don't report, which is something that we found here, or those who reported late, some of them almost 3 months late? And the situation where IGs are commenting or evaluating on an entirely different subsection than what the agency is reporting on? Is that something that is problematic for OMB? It was problematic for us in preparing our scores.

Ms. EVANS. We are working with the IGs. There is an IG Council similar to the CIO Council of which my boss Clay Johnson also is the chair of. We have started meetings with the IG to actually deal with a lot of those types of issues about resolving what are the differences in the interpretations of the way that certain things are written in there so that when you get a report again how an IG is evaluating, it would be consistent, and it gets back to the same issues of their interpretation of the metrics and the agency's interpretation of the reporting as well.

Those meetings have begun. We are working to get their input into this process so that when we issue the FISMA guidance for this year, we hope to bring clarity to those issues so that things will be more level, so to speak, between the IGs.

Mr. PUTNAM. That would be very helpful.

Mr. Dacey, what are your thoughts on that discrepancy between the IG reports and the agency reports? Has the GAO made any recommendations on how we can improve the audit process?

Mr. DACEY. There are a couple of things that I think need to be considered moving forward; and I would agree, too, that the meas-

ures need to—I'm not saying the measures that are here but additional information perhaps is a better way to describe it. It may be helpful to interpret the progress of agencies and information security.

When FISMA was set up, I think an important part of that was to have the IGs be an integral part of the process for a couple of reasons.

First of all, I think they provide a valuable independent check on the security of the systems. In other words, if we're looking at a system as we do, GAO, when we look at systems, we may identify vulnerabilities. The first question we ask is, well, have these been picked up by the agency's CNA process, if there was a CNA done. Had they been picked up in the plans of actions and milestones and things of that nature? If we find that they haven't, then we know something is broken and something isn't working right. It's kind of definitive proof that at the end of the day process was or wasn't working. So I think that's an important role.

The role that I think needs to evolve, though, is to get the IGs more involved in looking at the processes by which the agencies develop these numbers and the way they report them. I think if they do that and there is a process that is relatively reliable in bringing those numbers forward—and I focus on that, too, because oftentimes the numbers aren't available until the very end, so auditing the numbers themselves may be a challenge. So I think the IGs can look at the process and match that up again when they're doing their audits. If they are auditing a system and it hasn't been CNA'd properly but yet the agency is counting it in their CNA tally, then that is a problem.

So I think you need to work to keep that going, but again kind of increase the IG's roll to look at the processes and match that up against what they're finding in the individual systems that they do audit.

Mr. PUTNAM. Ms. Evans, there is an article in today's Washington Post where a Federal judge has ordered the Interior Department to shut down most employees' Internet access and some of the public Web sites, "after concluding that the agency has failed to fix computer security problems that threaten millions of dollars owed to Native Americans."

I understand that this is an ongoing issue, but if you would like to comment on it, I would like to give you that opportunity.

Ms. EVANS. Well, my only comment would be—is that Interior, just like any other department, is that we continue to work with them to assist them in addressing what their cyber security issues are through our processes like the President's management agenda, the scorecard, as well as the budget process that we just recently talked about in that guidance.

Mr. PUTNAM. What did Interior get? What was their score, their grade?

Ms. EVANS. An F.

Mr. PUTNAM. Is there any other department that—I mean, when we talk about computer security, sometimes we get off in the weeds, and it almost becomes this academic discussion. I mean, I have never heard of a judge ordering somebody to disconnect from the Web. Has that ever happened before?

Mr. Dacey.

Mr. DACEY. This is actually the third time for Interior, I believe, that an order has been issued by the court to stop. That's the only one with which I'm familiar at a Federal agency where there has actually been a court involvement in the process.

Mr. PUTNAM. So it's so bad that three times the judge has ordered them to disconnect?

Mr. DACEY. Well, not speaking to the individual case, but there is a legal case in dispute, and the judge, in ruling on that, in protecting the reliability of certain data that related to the Indian Affairs that they are concerned about people being able to get in. In fact, I believe at the first go around, when they were removed, the court had hired an ethical hacking group to participate, and they, in fact, had broken into their systems. And I believe it was reported that they created fictitious accounts in the Indian Affairs systems. And that became the concern, that you needed to protect access from outside into this data and this financial information related to that.

I would note that Interior, though, even on the measures that are on OMB's scorecard, pretty much consistently, except for one area, was below the average of other Federal agencies and, as you said, got an F in their grade. So there is a challenge there, I think, in their information security.

Mr. PUTNAM. I would say so.

Mr. Dacey, you mentioned in your report, the CIO's don't control mission systems. And I believe I read in Ms. Evans' testimony that, in fact, 65 percent of IT is mission-related activities. I thought FISMA put CIOs in the position of responsibility for all agency systems. Could you clarify that?

Mr. DACEY. I guess—I think our reference was actually to what OMB had said, so I will let Ms. Evans take care of that. But at the same time, I think it is important to note that—and I don't have an exact count, but one of the challenges is also making sure that authority goes with that responsibility. I know an increasing number of agencies has clearly given their CIOs the authority to enforce security standards throughout the agency. I don't have numbers, but I do believe that some do not have that authority. And in fact, I know when we have been doing some of these audits, we found that, in fact, the CIO at the agency level didn't always have control over what the individual bureaus did which could endanger security of the entire agency if not properly controlled. So I think that is one aspect. But, again, Ms. Evans might want to talk more about the specific numbers.

Ms. EVANS. You want to understand how it works?

Mr. PUTNAM. Are CIOs responsible for the mission-related activities or not?

Ms. EVANS. They are responsible from a strategic standpoint and from a corporate standpoint, which means that when an agency is divided off or a department is divided off and you have the offices within it, you get the guidance from headquarters, so to speak. And so the CIO is responsible for formulating what is that overall guidance, what is that policy, to ensure the cyber security going forward for that department.

When the program office—and in this case, we are talking agency senior officials—when they send their investment plans forward and they have an operational aspect of what they are doing within their program offices, they have to adhere to those policies and guidelines. And then the CIO, if they have an operational aspect, can ensure that they are conforming to those policies.

Sometimes some CIOs only have a policy aspect. If they have the policy aspect, then they are involved through the budget process to ensure all of these other things that we are talking about—that the investment has adequate cyber security based into its life cycle, that they do have plans that are in place that continue to measure what is going on within their program offices. So they do it from a corporate perspective.

If they have an operational perspective, that is an additional authority suit because, normally, what they do is they control infrastructure as well as telecommunications, all of those types of things. So they control the big network. So they can put policies in place that say, if you don't meet this certain threshold of security or if you are not certified and accredited, you cannot hook up to departmental resources. And that's usually where most program offices need to go in order to be able to go out to get onto the Internet to be able to reach, you know, big financial management types of systems, HR systems. And so CIOs do have the authority to be able to do that if they manage the corporate assets.

Mr. PUTNAM. Have you had an opportunity to read the GAO report that they released today, Ms. Evans?

Ms. EVANS. Well, we were glancing at it today.

Mr. PUTNAM. The breakdown of all the different information security measures and their taxonomic chart is pretty darned good. You came from Energy and from Justice as a CIO, you understand the challenges both from your current level and from the agency level perspective. And we are going to photocopy the key portions of that GAO report. We have to take the blue binder. Because of the blue binder, nobody is going to read it. But we have to really kind of break it down into the easy-to-understand key charts that Mr. Dacey put together.

If you were going to send it to somebody in the agency to bring about change, who would you send it to, because CIOs already know that stuff? I mean, they could have written it. I mean, when you are talking about kind of an easy-to-use, easy-to-read user's guide, who would you send it to really have an impact on behavior and understanding of what we are talking about in making systems more secure?

Ms. EVANS. In this particular case, if I put it in easy-to-read key charts off of here, we work—the initiative owners through the President's management agenda work very closely with the President's Management Council. So I would send it out through the President's Management Council and say, here is a guide of—here is what you need to look at as technologies are coming up. Because the CIO advises that person as the chief operating officer of the agency, most times it is the deputy secretary of the department that participates in the President's Management Council.

Mr. PUTNAM. And that's the person who also makes the decisions about what budget requests to send to you, about whether we are

going to buy this system or that system and we are going to have a firewall or a VPN or who gets——

Ms. EVANS. They review—deputy secretaries review the budget as they come up. Most agencies have hearings in the summer based on the guidance that goes out. And the key offices, just like a CIO, have input into how a program office is put together, how the budget is put together, recommendations. And so if there are issues—say, for example, based on my days at Energy, if there were issues with a specific program office who we felt really wasn't pulling their weight as far as cyber security was concerned, when these reviews occur, the deputy secretary would get key questions to ask that assistant secretary during their review.

You know, one question could be, how well are you working with your CIO? You know, do you have everything in place? Are you ensuring that cyber security is being adequately addressed within your program office?

And so something like this, if it was dealing with investment decisions and these would be key points, those would be like key questions that you would ask them so that they could ask to ensure that their portfolio, when it comes forward, meets those criteria.

Mr. PUTNAM. Thank you.

Mr. Wu, FISMA made NIST responsible for issuing a fair amount of guidance, guidance that is essential to the security of the information systems in the Federal Government. Could you comment on—and you did somewhat in your opening statement—could you elaborate on the resources that are necessary to provide that guidance?

Mr. WU. Well, certainly at the Department of Commerce and also at NIST, there is an understanding of the importance of NIST's role in implementing FISMA in how general standards are developed and created, and the key role this plays as the linchpin, the first domino, in a sense, for FISMA to be implemented very effectively. And so there is a priority placed within the Computer Security Division and within our Information Technology Laboratory to make sure that we meet all of the mandates and requirements of FISMA.

The challenges I alluded to in my testimony and Bob referenced in his is that, at least for this fiscal year, NIST did not receive the President's budget request for 2004; Congress was unable to provide that. And as a consequence, there is a fear that we may not be able to move forward in some of the research that would be required for some of the more emerging technologies.

For example, as we focused on a very real and immediate near-term need for guidance under FISMA, we are not keeping up with the rapid advances and technologies like RFIDs, the Radio Frequency Identification Devices, which is a very key component to some of these emerging technologies for communications that, unfortunately, under our funding situation, we may not be able to put resources in there for—certainly for 2004. We have to delay it for 2005 depending on how the congressional appropriations may look.

So there is a fear and a concern within the laboratory within the Department that we may not be able to be as aggressive as we'd like to be in our efforts and research. But in terms of meeting the FISMA responsibilities, NIST is committed to doing that.

Mr. PUTNAM. And the guide that you are creating for FISMA, I would imagine, would be pretty helpful guidance outside the government as well. Does NIST have an ability or a system to allow people to download that guide or to have access to that guide, to request it so that there can be a wider distribution?

Mr. WU. Well, information dissemination is critical to make sure that the work that NIST does is brought out to the Federal agencies as well as to the private sector. But it does have a cost as well. We hope to work very closely with OMB as well as with NTIS, which is also part of the Department of Commerce, for information dissemination so that we can have the information placed in as many hands as possible. And also NIST will, of course, make it available on its Web site.

Mr. PUTNAM. FISMA also requires agencies to develop policies governing configuration, so if someone sets up a server, they know what security controls they have to set, and NIST has developed that guide as well. What is the status of that?

Mr. WU. The status of—I believe—I'm not quite sure which—if you are referring to a specific publication or a specific—or a publication number. But we can certainly provide that for you.

Mr. PUTNAM. Thank you.

Mr. WU. But as I said, right now, NIST has met its timeliness requirements for its publications, and we look forward to completing those if—either in right now or available in public draft or available in terms of a full report.

Mr. PUTNAM. Ms. Evans, is there, for lack of a better term, a rapid-response team of professionals who can move into a situation like this Department of the Interior issue and work to resolve it on an emergency-type basis? I mean, recognizing, in addition to just being terribly embarrassing, it has cost people money and defrauded the Government and everything else. The fact that it has happened three times is—what is OMB's role in a situation like that?

Ms. EVANS. Well, each agency is responsible for having a computer-assistance-type team, incident-response team. However, through the new work that is going on now over at DHS—my office works very closely with DHS, especially in the area of implementation of the National Cyber Security Strategy. And so with working with the particular office over there under IAIP and working with those groups, there are several resources that they put in place that work very closely in conjunction with the CIO counsel. So in a particular situation like this, we could make recommendations as well as DHS could make recommendations of getting specific assistance through the resources that are available at DHS.

Mr. WU. Mr. Chairman, if I may, I was just handed some information. As Ms. Evans mentioned about DHS, we have also been working with DHS. And in regard to your question about the comprehensive security checklist and benchmarks, DHS has been partnering with NIST in this regard, and we will be able to maintain a Web-based portal on this listed checklist. And we hope to have that available in fiscal year 2005, in the years after as well.

Mr. PUTNAM. Very good.

Mr. Dacey, would you comment on the 2003 FISMA reports, the areas that strike you as being the most important improvements,

the most important deficiencies and your evaluation of the progress overall?

Mr. DACEY. Well, I think in my oral statement I raised some of the concerns. I know there has been progress. We have seen evidence of that through increases in the measures. But we have also seen that through looking at the whole series of audits that have taken place, both in respect to financial audits and other audits that the IGs have performed and GAOs performed. So there are improvements. I would characterize them as kind of heightened awareness as well or continued heightened awareness by agencies for a couple of reasons: A, they know we are not going away. This is an annual event, in fact now quarterly, reporting to OMB. So I think that is an important issue.

So there is a recognition that things are going to be watched. And, of course, the involvement of this committee is an important element in that as well.

In terms of the areas that are the concerns, I guess, or some of the areas of concern would be trying to make sure that some of these percentages keep increasing. And the pace of that is a good question. And how fast they can increase, I can't tell you. But certainly they have been improving over years. But the areas that are of concern most in my mind would be the certification and accreditation and the control testing, because that's where you are going to identify whether there are additional weaknesses and vulnerabilities in your system. If that is done correctly is, I would say, most important and certainly key, because that may unveil additional weaknesses that need to be addressed that haven't been identified yet.

In terms of the contingency planning, I have spoken about that in my statement as well. That is a critical area. And we have, again, less than half of the agencies with tested plans. And NASA, actually, has quite a bit of success in their reporting of that measure. If you exclude NASA, I think it is around 38 percent/40 percent of agencies that have tested plans, the rest of the Federal Government. So I think that is an important area because I think as we have increased exposures to viruses, worms and other kinds of malicious attacks, you really need a contingency plan in place, because I'm not sure you can anticipate everything that might happen to your system, particularly when we are getting to a time when it is conceivable that attacks could be launched before vulnerabilities are notified and identified in the public and patches are even made available. And that is definitely a trend.

So I think that is another area of importance. Some of the agencies are literally, I think, at zero percent on their contingency plan testing—and some very low. So I think those are some areas that kind of jump out in my mind when I look at the FISMA reports.

Again, in the progress area, I think it is important to keep having OMB managing and monitoring the process, Congress involved, the IG's involved. There are a lot of players.

I think the other key area would be to have the agencies make sure they have the processes in place to manage this on an ongoing basis. Two or 3 years ago, I'm not sure anybody really had a whole lot of processes in place. When we had the first GISRA reports, it was extremely ad hoc reporting that was coming into the agencies,

and they were putting it all together—and Karen can speak to that and how it was at Energy. But it wasn't a pretty process.

And as time has gone on, some of the agencies have developed more routine processes to get that information, to manage it day to day, not just for FISMA reporting purposes or for GISRA but actually to use it from a management standpoint. I think that is going to be a critical role in changing this whole dynamic and moving to a more sustainable progress that goes forward.

Mr. PUTNAM. That has been one of the complaints, is that agencies and their CIOs, in preparing their reports, they are really only trying to just meet the requirements of FISMA, and they are not actually improving the overall information security.

And I suppose that gets to your earlier point, Ms. Evans, about the next level is making more meaningful, more mature, as you put it, requirements.

Ms. EVANS. Right.

Mr. PUTNAM. Did you want to add anything in terms of your evaluation of the scores and progress, deficiencies, thoughts?

Ms. EVANS. Well, again, I would just like to say that we are making progress. I mean, we couldn't even give you—even though we don't have a real good solid way of doing the inventory, we couldn't even give you these numbers previously. I mean, we couldn't even—we would be debating on what is a system and how to move forward. So I think the government has made huge progress.

And although we are looking at these reports, I think you can also demonstrate, based on the results, that the Government is moving forward. And that is our ability to repel attacks as they are coming about and to deal with services as viruses are occurring.

Two or 3 years ago, when you looked at what we were doing when Corea came out of Melissa, many of the agency systems went down, and they were offline. And that's why they had to have contingency plans and everything else. But now, with the viruses that appear to be coming out, sometimes hourly, the agencies are being able to sustain business and being able to go forward because these processes are in place. They are looking at things. They may not be the best. There is a lot more that we can do, but we have made progress.

Mr. PUTNAM. Am I overemphasizing this inventory issue? I mean, in terms of the big scheme of things and government information security, am I too hung up on that? I mean, in terms of the priorities, the problems that are out there?

Mr. DACEY. I don't think you are too hung up on it. I think there's several reasons. First of all—I mean, not just because it can affect some of the measures, because denominators are going to change dramatically, particularly when DOD's numbers come into play, it will change dramatically.

But the issue is how to manage the systems. I think there are a lot of cascading effects. I know when we started looking at some of the patch management practices, one of the challenges in doing that was even identifying the systems they had so they can figure out, well, does this patch apply to me?

A lot of agencies defaulted to system administrators individually having to try to deal with that. And I know we had the issue with PADC and tried to put out something at a Federal level to help

agencies at least notify them. But the lack of a real complete inventory was a challenge, because we had several agencies that said we want PADC for every system administrator because, otherwise, we don't know collectively at the top what all our systems are, and you are going to have to deal directly with them.

It also affects configuration management. I don't know how you manage your configuration if you don't know what all your pieces are.

So there is a lot of additional cost and cascading effects. So, no, I don't think it is a light issue; I think it is a serious issue, again, mainly because it relates to these other areas that really can't be performed well or efficiently without it.

Mr. PUTNAM. There are a lot of Fs. How much difference is there within the F category? Are there some that are on their way out of the F category? I mean, are all the Fs grouped together, or are there some that are just off-the-chart bad, like Interior? I mean, three judges' orders to shut down the Internet is pretty—I would think would be about as bad as it gets. But maybe it really is worse. I don't know. I'm scared to know the answer.

Mr. DACEY. One thing that we also tried to look at in our analysis of the information was across the seven performance measures that are detailed in OMB's reports is, how are agencies doing relative to the average for those measures? In other words, how are they doing? And we found there were—let's see—seven agencies that were below in all seven measures, or at least one measure, or maybe one measure was above and six below. So there are some agencies where there is a pretty consistent below average score across those measures, and I think that carries into some of the other things that were considered in your grades as well.

At the same time, there are people at the top level, too, that are consistently—we have, let's see, eight agencies that are above average in all categories or all but one.

So you have a lot of players at both ends, and then you have a whole bunch of agencies in the middle. So I think it is a mixed story. And even within some agencies, they might have several above and several below. So it is not an even kind of process in bringing them up necessarily.

Mr. PUTNAM. How many—in that lower category, how many below average ratings did the Department of Defense have?

Mr. DACEY. The Department of Defense actually, based on the information I have, was—exceeded the average in five of the seven categories.

Mr. PUTNAM. But still received an F?

Mr. DACEY. Yes. There was a general correlation between the seven measures against the average and the grades. There are a few anomalies, because the grades the subcommittee gave included a consideration of a variety of other FISMA indicators that weren't part of these seven factors. So there are some. But in general, they tended to be in the same relative range.

Mr. PUTNAM. And DOD was allowed to report on a subsection of their systems. Correct?

Mr. DACEY. That is correct.

Mr. PUTNAM. Is any other agency given that consideration?

Mr. DACEY. Other than the stipulation that a lot of agencies don't have complete inventories, which is obviously a problem.

Mr. PUTNAM. All but five are reporting on a portion of their systems.

Mr. DACEY. They are the only agency who has reported or acknowledged that they are only reporting on a subset of their whole systems. I think they have 3,000 or 4,000 systems in total.

Mr. PUTNAM. And next year, they will be required to report on all.

Mr. DACEY. I will defer to Ms. Evans. That's what was in their report.

Ms. EVANS. Right. And on the scorecard, going forward on the scorecard, which we are referring back to, they are required, in order to be able to move, if they want to move to green, just like all agencies, they are required to report on all. And we are holding to that criteria.

Mr. PUTNAM. But, I mean, other than not being a green in the President's management report.

Ms. EVANS. Well, you have to look at this. This is still a management issue. These are very highly competitive folks. And this gets back into, you know, when the scorecard gets published, and it is just like this scorecard here, I mean, nobody wants to be an F. And so you are either going to rationalize why you are doing badly, or you are just going to improve your processes overall and move forward.

The whole purpose of the President's management agenda is to achieve results, and the President is very committed to that, and this administration is very committed to that. This is a piece of that agenda. And so we are committed to achieving the results, and the results are to ensure that we have a good cyber security posture going forward. So that is how we intend to hold the agencies accountable.

Mr. WU. Mr. Chairman.

Mr. PUTNAM. I hope you are right.

Mr. WU. At the Department of Commerce, we, as Ms. Evans has indicated, are striving to try to reach green. And it is a competitive process. Secretary Evans has made that a priority, and I suspect all the other secretaries have as well. We haven't quite reached it yet, but we are making strides, and we do want to do that. And so there is a commitment to do that, and we are following the guidance of OMB and Ms. Evans.

Mr. PUTNAM. Well, I hope NIST got a good score.

Mr. WU. Well, NIST is part of the Department of Commerce.

Mr. PUTNAM. What did Commerce get? I don't have it in front of me. A gentleman's C?

Mr. WU. No, I think we did well. I will have to talk to our Inspector General.

Mr. PUTNAM. You got a C.

Mr. WU. I will speak to Johnny Frazier and see how much better we did.

Mr. PUTNAM. C for Commerce.

All right. Any other comments from our first panel before we move into the second half of this hearing? I want to thank all of you for your participation and your ongoing efforts to improve this.

It is a long, hard struggle, and I know most of you have been in it for a whole lot longer than I have. And I tip my hat to you, and I wish you the best as we continue to move forward. And we certainly offer the resources and the abilities of this subcommittee to help you help them do a better job. Thank you very much.

And we will stand in recess for a couple of minutes until we can set up the second panel.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene. We have seated panel two. As is the custom with this subcommittee and the full committee, I would ask the witnesses and anyone accompanying them who will be providing information to please rise and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. Let the record note that all four witnesses responded in the affirmative.

We have had a request from the NRC to use a photographer. Since they are one of only two who got an A, they can have whatever they want. So come get a picture of this big smile.

We will begin our testimony. The first witness is Paul Corts. Paul R. Corts was sworn in as Assistant Attorney General for Administration in November 2002. Prior to entering government service, he served as president of Palm Beach Atlantic University for 11.5 years. He also served as president of Wingate University in North Carolina and has held administrative and teaching positions at Oklahoma Baptist University and Western Kentucky University. As Assistant Attorney General for Administration, Dr. Corts oversees the Department's Justice Management Division and is the chief financial officer.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF PAUL CORTS, ASSISTANT ATTORNEY GENERAL FOR ADMINISTRATION, DEPARTMENT OF JUSTICE

Mr. CORTS. Mr. Chairman, I appreciate the opportunity to appear before you today to discuss the Department's efforts in the areas of information technology security and the actions underway within the Department to institutionalize the daily management of security risks and to implement the requirements of FISMA. And I want to commend you and the committee for your past and current efforts to shine the spotlight on Federal agencies' security performance.

I certainly want to emphasize that the Department of Justice embraces the importance of IT security. Our senior management is committed to protecting the Department's IT assets from attacks and vulnerabilities, and we have clearly identified responsibility for IT security with the CIO.

IT is key to the Department's success in meeting our strategic goals. We place a very high value on the availability and integrity of the information in our systems, along with confidentiality and privacy concerns. And the nature of our work in Justice requires a highly robust security for IT.

As reported in the OMB Security Act Report for 2003, we reported 243 IT systems, 24 programs, 35 contractor operations and facilities. All of our programs and 206 systems were reviewed in ac-

cordance with FISMA guidance provided by OMB and NIST. The Department incorporates IT security requirements in all of our contracts, and we perform security reviews on half of the contract operations and facilities during the fiscal year. In addition, over 90 percent of our IT systems have been assessed for risks, and over 80 percent have been fully certified and accredited to date.

In the past, the Department operated in an extremely decentralized fashion, and that really contributed to IT and the computing environment being highly fragmented. This is a major concern with our inspector general during the past years, and since we joined the Department, it is a concern that the CIO and I share. Furthermore, we are fully aware of your concerns with our progress in information security, and we take these very seriously as well.

Since I arrived at Justice 16 months ago, the Department has taken a number of actions that not only reflect the commitment of senior management to correcting past deficiencies but also to establish a solid foundation for sustained future progress. And many of the IG's recommendations have been accomplished, or initiatives are underway that will provide for improved performance in the coming year.

Through the AG's leadership and vision, I think we have come a long way toward a more centrally coordinated department, and this has made a lot of progress and a very positive impact on our IT efforts.

Specifically, we have clarified our CIO position in terms of the Clinger-Cohen Act responsibilities, we have implemented a Web-based security awareness training tool. We have trained 77 percent of our employees so far on that with a goal of 95 by summer, implemented a computer emergency response team and integrated IT security with a capital investment process and some other actions that are underway to remedy deficiencies.

The Department's senior management team is committed to ensuring that these activities are under way, and we have them planned to correct both past deficiencies and be sure that we integrate these into an institutionalized kind of an environment.

We have reorganized the office of the CIO and named a chief information security officer. We've developed a Department-wide IT security program. We have established IT security program goals. We have approved a policy for 17 information security standards; chartered an IT Security Council and six project teams; integrated IT security with enterprise architecture and the investment management process, developed system risk assessment and a test plan tool; provided for CIO collaboration and review of component corrective action plans; continued development of a public key infrastructure capability; continued development of a unified financial management system throughout the Department; provided resources to assist components in assessing their systems; implemented a monthly report card, which you see here.

This is the age of the report card. So we've come up with a report card, a sample there, that is done on a monthly basis to let the individual components know how they are doing in the area of IT security.

So the accomplishments and initiatives we have underway address many of the IG's recommendations and will provide for im-

proved performance in the coming year. We acknowledge the need to do more. It is a matter of continuous improvement that we are committed to while at the same time we are working to reduce risks associated with our IT assets. And I want to thank you and the committee for the focus that you are giving to this, and we pledge to you our cooperation and support.

[The prepared statement of Mr. Corts follows:]

Statement of
Dr. Paul R. Corts
Assistant Attorney General for Administration
U.S. Department of Justice
Before the
Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
U.S. House of Representatives
March 16, 2004

Mr. Chairman, Members of the Subcommittee:

I appreciate the opportunity to appear before you today to discuss the Department's efforts in the areas of information technology (IT) security and the efforts underway within the Department to institutionalize the daily management of information security risks and implement the requirements of the Federal Information Security Management Act. I would like to commend you and the Committee for your past and current efforts to shine the spotlight on Federal agency and security performance.

I wish to emphasize at the outset that the Department of Justice (DOJ) recognizes the importance of IT security and the Department's senior management is committed to fully protecting the Department's IT assets from attacks and vulnerabilities. I further wish to emphasize that responsibility for the Department's IT security program rests with the Department's Chief Information Officer (CIO).

Information technology (IT) is key to the Department's success in meeting our strategic goals. It provides new and improved capabilities to gather, analyze, and share intelligence information; identify, monitor, apprehend, and prosecute terrorist or criminal suspects; identify and prevent persons who are national security threats from entering the United States; securely share information with our federal, state, and local partners; efficiently manage our criminal and civil cases; provide accessible, speedy, and reliable services to our customers; and efficiently and effectively carryout our internal business practices. In addition, it provides the communications and computing infrastructure that ensures continuity of operations and rapid response in times of crisis.

The integrity and availability, and where appropriate the confidentiality and privacy of the information in our systems are today more important than ever. The value of computer and telecommunication systems and the vital information they process and transport became even more apparent in the wake of the tragic events of September 11th, 2001.

In the past, the Department operated in a very decentralized manner, and the IT computing environment and our IT security program was further fragmented within the Department. This has been a major concern with our Inspector General (IG) during the past years and has hampered mission accomplishment. Furthermore, we are fully aware of your concerns with our progress in information security and we take these concerns seriously.

Since I arrived at the Department of Justice 16 months ago, the Department has taken a number of actions that not only reflect the commitment of present management to correcting past deficiencies but also establish a solid foundation for sustained future progress. The accomplishments and initiatives we have underway address many of the IG's recommendations and will provide for improved performance in the coming year.

The current state of IT Security within the Department

The Department's IT security budget for FY 2004 comprises 3.7% of the planned IT portfolio of $2,074 million. In FY 2003, we reported 253 IT systems, 24 programs, and 35 contractor operations and facilities. All of our programs and 206 (81%) systems were reviewed in accordance with the FISMA guidance provided by OMB and the National Institute of Standards and Technology (NIST). The Department incorporates IT security requirements in all of our contracts and further reviewed half of the contractor operations and facilities during the fiscal year. In addition, over 90% of our IT systems have been assessed for risks and over 80% have been fully certified and accredited to date.

In FY 2003, the Department implemented a web based computer security awareness training tool, to provide all employees and contractor personnel with access to Department systems basic end-user security training. During the first nine months of operation, we trained 77% of our employees and we stand committed to ensuring all employees and contractors receive basic security awareness training and that privileged users, such as system and network administrators and security professionals, receive specialized training.

The Department operates a computer emergency response team and has developed standards for reporting incidents within the Department. This group serves as the single point of contact to FedCIRC and verifies patch implementation at components. We are also working with the Department of Homeland Security to utilize their Project Matrix methodology to ensure the proper identification of our mission and national critical operations and assets. We are further committed to ensuring all of our systems have contingency plans in place and that these plans are tested at least annually.

Our CIO reports directly to the Attorney General for his duties and responsibilities identified by the Clinger-Cohen Act. Our CIO also serves as the Deputy Assistant Attorney General for Information Resources Management and is a vital part of our Departmental management team, and routinely coordinates IT initiatives and

programs through my office and with me as the Chief Financial Officer and the Procurement Executive.

Through the Attorney General's leadership and vision, we have come a long way toward a more centrally coordinated Department, and this has made a very positive impact on our total IT efforts.

In June of 2003, the CIO established an IT Security Office to oversee the implementation of the Department's IT Security Program, led by the chief information security officer. In November 2003, I signed a Departmental Order clarifying the CIO authority and responsibilities for IT security. This single point of authority for information security program management and oversight implements the IG's recommendation to provide a central IT security office. This office is responsible for developing IT security policy and standards, and has organized a security council comprised of top security officials from each of the Department's component organizations. In addition, our IT Security Office coordinates with other security programs, including personnel and physical security.

The Department has integrated IT security within the capital investment process and the system development life cycle. We are continuing to develop a security architecture as an integrated element of our enterprise architecture, so that the IT investment process and our future infrastructures adequately incorporate our security needs and prevent IT security failures in the future.

In addition to the strategic improvements identified above, we have been addressing many of our known weaknesses within our current operations through our curative efforts. These efforts include certifying and accrediting our legacy systems, identifying vulnerabilities and weaknesses through regular risks assessments and testing of security controls. In addition, we have been implementing near term fixes and monitoring corrective plans of actions and milestones (POA&Ms) to provide for an overall net reduction in risk.

In our FY 2003 Accountability Report, we reported two material weaknesses relating to IT security, one of which is a Department level material weakness relating to component implementation of management, operational, and technical security controls and the other is specific to securing the FBI's infrastructure and implementing an IT security program. Both material weaknesses are from the previous year and have associated plans of actions and milestones to manage corrective action.

Actions underway to remedy deficiencies in IT security reported in FISMA and financial reporting

IT security is a high priority within our Department. Accountability and responsibility is critical to our successful remediation of identified vulnerabilities and weaknesses. The Department's senior management team is committed to ensuring

activities are underway and planned to correct past deficiencies and to ensure future practices are institutionalized.

In addition to the many strategic initiatives identified previously, we have identified additional initiatives to further address the program and system level weaknesses identified in our FISMA and financial management reporting. At the program level we have:

- Developed a Department-wide IT Security Program to assess and reduce risk;
- Established IT security program goals;
- Identified program level resources;
- Approved policy and 17 information security standards for management, operational, and technical control requirements;
- Chartered an IT Security Council and six project teams to manage implementation and assist operational managers;
- Developed a Department-wide information security training and awareness program; and
- Implemented a monthly report card for monitoring component progress.

And at the system level we have:

- Integrated IT security with the enterprise architecture and investment management processes;
- Scheduled to achieve full approval to operate for 90% of all IT systems by July 2004;
- Developed system risk assessment and test plan tool incorporating over 250 management, operational and technical risk control requirements;
- Scheduled periodic validation testing to be completed by July 2004; and
- Developed a process for planning, resourcing, implementing and maintaining risk control requirements.

Additionally we have:

- Provided for CIO collaboration and review of Component corrective action plans;
- Implemented an initial capability for an integrated Department-wide tool used for documenting and evaluating system security controls and risk management and monitoring program and system corrective POA&Ms;
- Continued development of a public key infrastructure capability to support enhanced authentication controls and strategic initiatives in information sharing;
- Continued development of a unified financial management system across the Department that will incorporate the financial management and security practices; and
- Provided additional oversight and resources to assist troubled components in assessing their systems, developing POA&Ms, and ensuring development of certification and accreditation documentation.

Institutionalizing Information Security within the Department

As I previously stated, we have created a solid foundation for future implementation and effective management of information security across our Department. In July 2002, we issued the Department's Information Technology Strategic Plan. The plan, approved by the Department's Strategic Management Council (SMC), represents a starting point for what will be a long-term, sustained, and collaborative effort to significantly improve IT in our Department. We are focusing on four key areas: 1) IT infrastructure, 2) information security, 3) common solutions, and 4) management roles and processes. These four areas have been chosen because, together, they represent the core building blocks of the Department's IT program. Progress in implementing the IT Strategic Plan is monitored by my office in conjunction with the Strategic Management Council, on behalf of the Attorney General. Key management positions in the Office of the CIO are now filled with staff from the Senior Executive Service to lead the new organization in support of the Attorney General and the President's Management Agenda. The CIO continues to build the organizational capacity to carry out this ambitious mission as the new organization is implemented to support our IT strategy and operations.

I am pleased that we have been able to implement reorganization of our Department level IT organization. Among the main objectives of this reorganization was the elevation of the role of IT security, the enforcement of the importance of IT security, and the clarification of lines of responsibility and accountability. The reorganized Office of the CIO includes a senior information security official and establishes an IT security staff reporting directly to the Department's CIO. This staff is responsible for ensuring that all component systems have implemented the appropriate IT security controls, for ensuring that components identify POA&Ms when the security controls are not met, and for monitoring these corrective action plans. The new organization for the Office of the CIO was approved by the Attorney General, reviewed by the Office of Management and Budget (OMB) and the Congress, and implemented in May 2003.

The Department CIO has been working closely with component CIOs to ensure that program roles and responsibilities are defined and implemented. We are continuing to enhance and extend the use of standards and automated tools to help assess security controls and prioritize and monitor the implementation of corrective actions and to incorporate all known agency security weaknesses. We also are increasing our independent validation and monitoring of compliance with Departmental policy and practices, and ensuring that costs for security are identified in IT capital plans. At the same time, we continue to explore Department-wide infrastructure solutions that incorporate security and address crosscutting problems. For example, the Department is in the process of implementing a common telecommunications network that implements the security architecture for the wide area network and integrates many of the common security controls for the local computing environments.

We are also aggressively recruiting qualified IT security professionals to support system implementation and validation of security controls within our systems. We are

utilizing several unique government programs to strengthen our staff, which now includes direct hire authority for IT Security Professionals, and recruitment of Cyber Corps graduates and Presidential Management Fellows.

Furthermore, our Chief Information Security Officer has established a solid foundation for component integration with standards and procedures. We have implemented a monthly report card for each component to monitor performance. An example of the report card is summarized in the attached chart. Our overall objective is for our components to be green in each category and achieve full approval to operate on over 90% of our systems by October 2004.

The accomplishments and initiatives we have underway address many of the IG recommendations and will provide for improved performance in the coming year. We do acknowledge the need to demonstrate continuous improvement in our IT security program, while at the same time reduce the net risk associated with our IT assets.

I want to thank you and the Subcommittee for your continued focus on this important area. I would be pleased to take any questions at this time.

Mr. PUTNAM. Thank you very much, Mr. Corts.

Our next witness is Jeffrey Rush, Jr. Mr. Rush was sworn in as the Inspector General for the Department of Treasury in July 1999. Prior to that, he served as the Inspector General of the U.S. Agency for International Development and is the acting Inspector General of the Peace Corps. Mr. Rush also served for 23 years in the U.S. Department of Agriculture.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF JEFFREY RUSH, JR., INSPECTOR GENERAL, DEPARTMENT OF THE TREASURY

Mr. RUSH. Thank you, Mr. Chairman.

In your letter of February 26, you asked me to address three points in my statement: One, a summary of the state of information security at Treasury; two, the methodology used to audit Treasury and the resources available to my office; and, finally, the circumstances that led to the delay in our reporting of results under FISMA.

First, although we have been reporting on serious information security weaknesses since 1998, I will limit my testimony only to the work done in the last 3 years. Our reporting in fiscal years 2001 and 2002 was under the Government Information Security Reform Act [GISRA]. This most recent job was done under FISMA. All three assessments as well as management's own have identified serious deficiencies in information security throughout the Department.

Let me summarize just what we consider the important deficiencies to be. First, most of the systems have not been certified or accredited. Second, Treasury has been unable to provide an accurate inventory year to year of systems to be certified and accredited. Third, Treasury's plans of action and milestones and for fixing security—serious security weaknesses—are not complete and are inconsistent. Four, Treasury does not fully comply with the reporting of security incidents. Fifth, Treasury did not use the National Institute of Standards and Technology guidance for all of its programs. Sixth, interdependencies and relationships of critical operations have not been fully identified. And, finally, Treasury has not provided sufficient information technology and security training to the majority of its employees.

Second, in conducting our fiscal year 2003 evaluation of Treasury's information security program and practices, we follow the guidance issued by the Office of Management and Budget on August 6, 2003. I have attached a copy of that guidance to the statement. The guidance prescribed a set of questions to be answered by both agency management and by the Offices of Inspectors General. In this regard, OIGs were to evaluate a representative sample of all of the types of agency systems. One area that was to be emphasized this year was—in OIG's assessment—was against specific criteria which the agency developed, implemented or was managing in agency-wide plans of actions and milestones process. The plans of actions and milestones process is key to effective remediation of IT security weaknesses and instrumented for the agency to get green under the expanding government scorecard of the President's management agenda.

Finally, as background for the reason for our delay in FISMA reporting, during March 2003, we divested approximately 70 percent of our staff to the Department of Homeland Security Office of Inspector General pursuant to the Homeland Security Act. Our audit staff was reduced from 165 to 62 during the last 6 months of a fiscal year. Our annual audit plan had to be completely revised. Thus, this divestiture and subsequent attrition reduced our IT audit group from 14 to 5.

With our much reduced staffing, we determined we could not complete FISMA on schedule and sustain an accelerated audit of the Department's fiscal year 2003 financial statements. In consultation with the Department and the Office of Management and Budget, priority was given to the audit of the Department's fiscal year 2003 performance and accountability report, and we committed to issue the FISMA report within 30 days of that date. And, accordingly, the financial statement audit was completed on an accelerated basis on November 14, 2003, and we issued our FISMA report on December 15, 2003.

But let me stop and make clear to you that I probably owe you an apology. If not, I will give you one anyway. As early as July 2003, apparently everyone but this committee was informed of the decision to concentrate on completing the accelerated financial statement, clearly putting FISMA at a second priority; thus, the late report that was due in September.

Considering our current staffing levels and looking forward, we have not been able to and do not anticipate being able to hire additional IT auditors in the near future. Thus, we plan to contract for the FISMA evaluation for the non-national-security systems for fiscal year 2004. We will perform the fiscal year 2004 FISMA evaluation for Treasury's national security systems with our own staff.

That concludes my statement.

[The prepared statement of Mr. Rush follows:]

STATEMENT OF THE HONORABLE JEFFREY RUSH, JR.

INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,

INTERGOVERNMENTAL RELATIONS AND THE CENSUS

MARCH 10, 2004

Mr. Chairman, Ranking Member Clay, Members of the Subcommittee, thank you for the opportunity to testify in this hearing on "Information Security in the Federal Government: One Year into the Federal Information Security Management Act." In your letter of February 26, 2004, you asked me to address three points in my statement: (1) a summary of the state of information security at Treasury, (2) the methodology used to audit Treasury and the resources available to my office, and (3) the circumstances that led to the delay in reporting our results under the Federal Information Security Management Act (FISMA).

First, although we have been reporting on serious information security weaknesses since 1998, I will limit my testimony to work done in the past 3 years. This is the third year we have assessed the information security programs and practices in Treasury. Our reporting for Fiscal Years (FY) 2001 and 2002 was under the Government Information Security Reform Act (GISRA). All three assessments, as well as management's own assessments, have identified serious deficiencies in information security throughout the Department. We issued our most recent evaluation report pursuant to FISMA on December 15, 2003, and a separate, classified FISMA report on Treasury's national security systems on December 24, 2003. These deficiencies include:

- Most systems have not been certified and accredited.
- Treasury has been unable to provide an accurate inventory year-to-year of systems to be certified and accredited.
- Treasury's plans of action and milestones for fixing serious security weaknesses were not always complete or consistently reported on.
- Treasury does not have a fully functioning computer security incident response capability. In addition, the requirements for reporting incidents were not being applied consistently among Treasury offices and bureaus.
- Treasury did not use the National Institute of Standards and Technology's (NIST) guidance for all of its program and systems reviews. Other methodologies that Treasury used were not sufficient to substitute for the NIST requirements.

- Interdependencies and interrelationships of mission critical operations and assets were not fully identified.
- Treasury has not provided sufficient information technology (IT) security training to the majority of its employees.

At least some aspect of these weaknesses has been reported in each of the last 3 years. While some progress has been made, these weaknesses have largely gone uncorrected. In fact, in the critical area of certification and accreditation, Treasury's performance has declined.

With respect to certification and accreditation, for FY 2001, 18 percent of Treasury systems were certified and accredited; for FY 2002, 32 percent of Treasury systems were certified and accredited; and for FY 2003, 23 percent of Treasury systems were certified and accredited, Department-wide. It should be noted that the FY 2003 decline was significantly impacted by the number systems operated by the Internal Revenue Service (IRS) that were not certified and accredited. Not including the IRS systems, 69 percent were certified and accredited. Nevertheless, this matter has been further complicated by the Department's inability to provide an accurate inventory of its systems to be certified and accredited on a year-to-year basis. For example, in FY 2002 Treasury identified 626 systems requiring certification and accreditation; in FY 2003, Treasury identified 708 systems requiring certification and accreditation.

To its credit, Treasury management declared the lack of substantial compliance with information security requirements as a material weakness under the Federal Manager's Financial Integrity Act based on our FY 2002 evaluation. It continued to report this deficiency as a material weakness for FY 2003.

Second, in conducting our FY 2003 evaluation of Treasury's information security program and practices, we followed the guidance issued by the Office of Management and Budget (OMB) on August 6, 2003. For your reference, I have attached a copy of the guidance to this statement. The guidance prescribed a set of questions to be answered by both agency management and by the Offices of Inspector General (OIG). In this regard, OIGs were to evaluate a representative sample of all types of agency systems. FISMA also supports the OIGs' use of results of other IT-related reviews performed during the reporting period. One area that was emphasized this year was the OIGs' assessment, against specific criteria, of whether the agency developed, implemented, and was managing an agency-wide plan of action and milestones process. The plans of action and milestones process is key to effective remediation of IT security weaknesses and instrumental for an agency to get to "green" under the Expanding E-Government Scorecard of the President's Management Agenda.

For FY 2003, we participated with the Department's Office of Chief Information Officer and the Treasury Inspector General for Tax Administration in a joint data call to Treasury offices and bureaus. We performed limited verification of the data received. We also considered the results of our work performed during the year that directly impacted information security. For example, we observed a disaster recovery test for the Treasury Communications System and audited the Department's implementation of its critical infrastructure protection program. We also considered IT security audit work that was performed in connection with the audits of the Department and bureau FY 2003 financial statements.

Finally, as background to the reason for our delayed FISMA reporting, during March 2003, we divested approximately 70 percent of our staff to the Department of Homeland Security Office of Inspector General pursuant to the Homeland Security Act of 2002. Our audit staff was reduced from 165 to 62 during the last six months of the fiscal year. Our annual audit plan had to be completely revised. This divesture and subsequent attrition reduced our IT audit group from 14 to 5.

We had planned to complete our FISMA review by the OMB-prescribed deadline of September 22, 2003. However, with our much reduced staffing, we determined that we could not complete FISMA on schedule and sustain an accelerated audit of the Department's FY 2003 financial statements. In consultation with the Department and OMB, priority was given to our audit of the Department's FY 2003 financial statements, and we committed to issue our FISMA report 1 month later. Accordingly, the financial statement audit was completed on November 14, 2003, and we issued our FISMA report on December 15, 2003.

Considering our current staffing levels and looking forward, we have not been able, and do not anticipate being able to hire additional IT audit staff in the near future that would enable us to meet the anticipated FY 2004 FISMA reporting deadline. Thus, we plan to contract out the independent FY 2004 FISMA evaluation for non-national security systems. We will perform the FY 2004 FISMA evaluation for Treasury's national security systems with our staff. We also plan to perform audit work in certain key areas of vulnerability identified by our previous FISMA work. For example, we plan to audit Treasury's computer security incident response capability and conduct vulnerability scans of computer networks at selected bureaus. The results from these audit efforts, as well as any information security findings identified from our financial statement audits, will be integrated into our FISMA reporting for FY 2004.

This concludes my testimony. I would be pleased to answer any questions that the Committee may have. Thank you.

ATTACHMENT TO
TESTIMONY OF THE HONORABLE JEFFREY RUSH, JR.
INSPECTOR GENERAL, DEPARTMENT OF THE TREASURY
BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
MARCH 10, 2004

Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, dated August 6, 2003

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 6, 2003

THE DIRECTOR

M-03-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting

As you know, the security of the Federal government's information and information systems is a responsibility shared by every agency. The Administration's policy requires Federal agencies to take a risk-based, cost-effective approach to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats.

To assist Federal agencies in meeting their responsibilities, the President signed into law on December 17, 2002, the Electronic Government Act. Title III of this Act, the Federal Information Security Management Act (FISMA) along with OMB policy, lays out a framework for annual IT security reviews, reporting, and remediation planning. Under this framework, the Federal government is able to quantitatively determine both IT security progress and problems. This information is essential to ensuring that remediation efforts and IT resources are prioritized resulting in the timely resolution of IT security weaknesses.

This guidance provides direction to agencies on implementing FISMA and consists of the following four attachments:

- Attachment A – The information in this attachment is new and highlights the more substantive changes introduced by FISMA from previous IT security legislation.
- Attachment B – This attachment contains the FY03 FISMA reporting instructions for agencies and Inspectors General.
- Attachment C – This attachment contains directions for agencies on quarterly reporting on IT security efforts. It includes both the continued quarterly plan of action and milestones updates and performance measure updates.
- Attachment D – This attachment contains definitions in law and policy referenced in the guidance.

I would also like to take this opportunity to inform you of a number of actions OMB has undertaken to further assist agencies in improving their IT security status through the President's Management Agenda and the budget process. On a quarterly basis, agencies provide updates to OMB on their IT security efforts through quantitative performance measures and progress in remediating IT security weaknesses. This information is used to inform the agency's E-Government Scorecard under the President's Management Agenda.

Additionally, I am directing my staff to work with your agency to ensure that system remediation plans are implemented and appropriate resources are identified through the budget process to resolve critical IT security weaknesses.

Agency reports are due to OMB on September 22nd, 2003. Agency heads should transmit to OMB the agency report (containing both the agency and IG components) and copies of the IG's independent evaluations. This transmission represents a confirmation by the agency head of the agency's IT security status as detailed in the agency report. Your CIO and IG received an electronic copy of this guidance and templates to assist them in reporting. Agency reports will continue to serve as the primary basis for OMB's annual summary report to Congress.

A letter from the agency head that transmits the required information should be delivered to:

Joshua B. Bolten
OMB Director
Eisenhower Executive Office Building
Room 252
Washington, DC 20503

The agency reports along with copies of the independent evaluations and any other appropriate information should be sent electronically to Kamela White at kgwhite@omb.eop.gov. Instructions for submitting the quarterly IT security reports can be found in Attachment C.

Attachments

Table of Attachments

Attachment A – Transition from the Government Information Security Reform Act (GISRA) to the Federal Information Security Management Act (FISMA)

The information in this attachment is new and highlights the more substantive changes or additions introduced by FISMA from GISRA.

Attachment B – Reporting on Federal Government Information Security Management

This attachment contains the FY03 FISMA reporting instructions for agencies and IGs and a set of questions and answers to assist agencies and IGs. Most of the information in this attachment is identical to the FY02 reporting instructions, including the performance measures introduced in last year's guidance. One significant change directs IGs to assess against specific criteria, whether the agency has developed, implemented, and manages an agency-wide plan of action and milestones (POA&M) process. Additionally, there is a strong focus on performance measures to answer many of the questions and as a result the reporting instructions have been formatted to emphasize a quantitative rather than a narrative response.

Attachment C – Reporting on Remediation Efforts and Updating Performance Measures

This attachment contains directions for agencies on quarterly reporting on IT security efforts. This information is largely the same as in the FY02 guidance. It includes both the continued quarterly reporting of agency remediation efforts (through agency POA&Ms) and a new requirement for quarterly reporting of agency progress against a subset of the IT security performance measures in the FY03 reporting instructions.

Attachment D – Definitions

The definitions in this attachment are largely the same as those included in the FY02 GISRA guidance but have been updated to include new definitions introduced in FISMA.

This FY03 FISMA guidance and POA&M guidance replaces M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones").

ATTACHMENT A

TRANSITION FROM GOVERNMENT INFORMATION SECURITY REFORM ACT TO FEDERAL INFORMATION SECURITY MANAGEMENT ACT

On December 17th, 2002, the President signed into law the E-Government Act (P.L. 107-347) which includes Title III, the Federal Information Security Management Act (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA) which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as the development of minimum standards for agency systems. The National Institute of Standards and Technology (NIST) will work with agencies in the development of those standards per their statutory role in providing technical guidance to Federal agencies.

Please note that an earlier version of FISMA was enacted as part of the Homeland Security Act (P.L. 107-296). As provided in 44 U.S.C. 3549 and as stated by the President in his signing statement for the E-Government Act, the version of FISMA in the Homeland Security Act is not in effect. The version of FISMA in effect and to which all agencies are held accountable is the version found in the E-Government Act referenced above.

This attachment highlights the significant changes from GISRA to FISMA.

A. Definitions

1. FISMA introduces a statutory definition for information security. This definition is not substantively different than that used in current OMB and agency policies or NIST guidelines. Therefore, this new definition does not require changes to current policies or programs. It reads: "The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information."

All Federal information and information systems require some degree of security under one or more of the three elements of the forgoing definition.

2. Like GISRA, FISMA (section 3542(b)(3)) cites the Clinger-Cohen definition of IT which includes "equipment used by an executive agency directly or is used by a contractor under contract with the executive agency." However, FISMA's applicability is broadened by two other provisions.

First, section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Second, section 3544(b) requires that each agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

Thus, because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than that of prior security law. That is, agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc. FISMA therefore underscores longstanding OMB policy concerning sharing government information and interconnecting systems, i.e., Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III).

Finally, because FISMA applies to Federal information (in addition to information systems), in certain limited circumstances its requirements also apply to a specific class of information technology to which Clinger-Cohen did not, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal information is used within incidentally acquired equipment, the agency is responsible for ensuring that FISMA requirements are met.

B. Changes to annual reporting requirements

FISMA (section 3544(c)(1)) makes the following modifications to agencies' annual reporting requirements:

Annual reports under FISMA must now be sent to OMB and the Committees on Government Reform and Science of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, the authorization and appropriations committees for each individual agency of Congress, and GAO.

Because of this broader distribution, the agency reports should not contain internal Executive Branch predecisional, deliberative information. FISMA requires that OMB report to Congress no later than March 1, but does not prescribe a date by which agency reports must be sent. Agency reports (including the Inspector General's independent evaluation) are due to OMB on September 22, 2003. Agencies shall forward their reports to the appropriate Congressional Committees and GAO after the reports have been reviewed by OMB and OMB has notified the agency. Copies of the Inspector Generals independent evaluations may be released to Congress any time following their submission to OMB.

FISMA requires that each agency's report include information regarding: 1) agency risk assessments; 2) security policies and procedures; 3) subordinate plans (i.e., individual system security plans); 4) training; 5) annual testing and evaluation; 6) corrective action process; 7) security incident reporting; and 8) continuity of operations. Each of these categories fit into the existing reporting categories prescribed in OMB guidance and thus require no additional data gathering or reporting on the part of the agencies.

C. System configuration requirements determined by the agency
FISMA (section 3544(b)(2)(D)(iii)) requires that each agency develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.

OMB's reporting guidance will seek information on agency progress in meeting this new requirement, but for the first year will not judge the adequacy of that process.

One example to aid compliance with FISMA would be to employ the Windows 2000 configuration settings recently developed by NIST and NSA. Other configuration guides, for this and other operating systems and software applications are available or are also being developed by other sources and absent guidance from NIST could also be helpful. Agencies are reminded however, that OMB policy requires agency procedures be consistent with guidance issued by NIST when such is available.

Additionally, while many agencies have established patch authentication and distribution accounts through FedCIRC's government-wide patch management contract, actual usage of those accounts are extremely low. To ensure that agencies maintain up-to-date patches, it is critical that usage increase.

D. Annual testing and evaluation of security controls
FISMA (section 3544(b)(5)) requires each agency to perform for each system "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. . ." This evaluation will include the testing of management, operational, and technical controls.

This provision does not require annual testing of the complexity required for certification and accreditation of systems as described in NIST guidance. Rather, it recognizes the importance of maintaining a continuous process of assessing risk and ensuring that security controls maintain risk at an acceptable level. This provision also underscores the need to understand the security status of each system in order to accurately maintain system-level POA&Ms and report annually on the overall health of an agency's IT security program.

The necessary depth and breadth of an annual FISMA review depends on several factors such as: 1) the acceptable level of risk and magnitude of harm to the system or information; 2) the extent to which system configurations and settings are documented and continuously monitored; 3) the extent to which patch management is employed for the system; 4) the relative comprehensiveness of the most recent past review; and 5) the vintage of the most recent in-depth testing and evaluation as part of system certification and final accreditation.

For example, if in the previous year a system underwent a complete certification and received final (not interim) authority to operate, has documented configuration settings, employs automated scanning tools to monitor configurations, threats, and vulnerabilities, and has an effective patch management capability, a simple maintenance review using NIST's self assessment tool may meet the FISMA annual review requirement. If none or only some of the foregoing are true, then the annual testing and evaluation must be far more comprehensive commensurate with the acceptable level of risk and magnitude of harm. Agency officials must use sound judgment when determining the scope and rigor of FISMA's annual test and evaluations.

The flexibility described above does not alter OMB policy requiring system reauthorization (certification and accreditation) at least every three years or when significant changes are made, e.g., connecting to new systems or changes to configurations, hardware, or software. Agencies certification and accreditation processes must conform to NIST guidance. Additionally, the flexibility described does not dilute the statutory requirement that all systems must be reviewed annually.

E. Continuity of system operations

FISMA (section 3544(b)(8)) codifies a longstanding policy requirement that each agency's security program (and particularly each system security plan) include the provision for the continuity of operations for information systems that support the operations and assets of the agency. FISMA explicitly includes in this requirement, information and information systems "provided or managed by another agency, contractor, or other source." For the purposes of agency implementation, "other source" has the same meaning as "other organization on behalf of an agency" discussed above.

F. NIST Standards and Guidelines

FISMA (sections 302 and 303) directs the Department of Commerce through NIST to develop, subject to direction by the President and in coordination with OMB, compulsory and binding standards that will be used to "categorize all information and information systems collected or maintained by or on behalf of each agency".

As NIST develops these minimum requirements for standards and guidelines, agencies will have ample opportunity to review drafts and provide feedback and comments. OMB strongly encourages agencies to actively review and participate in these drafts. As these standards and guidelines are finalized OMB will issue, when necessary, accompanying implementing guidance for the NIST standards and guidelines.

G. Senior Agency Information Security Officer Responsibilities
FISMA (section 3544(a)(3)(A)(i-iv)) provides additional details on the responsibilities and qualifications of the senior agency information security officer. All agencies shall have a senior information security officer, designated by the agency CIO, who reports to the agency CIO. Commonly referred to as a chief information security officer this officer must: (1) carry out the CIO's IT security responsibilities; (2) possess professional qualifications, including training and experience, required to administer FISMA requirements; (3) have information security duties as that official's primary duty; and (4) head an office with the mission and resources to assist in ensuring agency compliance with FISMA.

H. Reporting of Significant Deficiencies
FISMA (section 3544(c)) provides additional detail regarding the reporting of significant deficiencies. Specifically, FISMA requires agencies to "report any significant deficiency in a policy, procedure, or practice identified [in agency reporting] – (A) as a material weakness in reporting under section 3512 of title 31; and (B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note)." Accordingly, agency heads must consider such significant deficiencies when providing assurance on controls under the Federal Managers Financial Integrity Act (FMFIA) and determining compliance with the Federal Financial Management Improvement Act (FFMIA).

I. Inventory of Major Information Systems
FISMA (section 305(c)) amends the Paperwork Reduction Act and requires the head of each agency to develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of "major information system" is found in OMB Circular A-130.

The FISMA amendments requires that the identification of information systems in this inventory include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. It is OMB's expectation that each agency should have such an inventory via its work on developing its enterprise architecture. The FISMA amendments also provide that the inventory be updated at least annually, made available to the Comptroller General when requested, and used to support information resources management including monitoring, testing and evaluation of information security controls.

ATTACHMENT B

REPORTING ON FEDERAL GOVERNMENT INFORMATION SECURITY MANAGEMENT

Attachment B consists of two parts:

- Part I – which provides reporting instructions and the format for developing the agency and IG reports.
- Part II – which provides a series of questions and answers to further assist agencies and IGs in meeting the annual review and reporting requirements.

In general, these instructions for reporting the results of FY03 FISMA reviews remain nearly identical to the FY02 instructions. Agencies are not requested to collect any new type of information. The two significant changes are an increased emphasis on performance measures and additional guidance to IGs to assess whether agencies have an agency-wide remediation process that meets OMB criteria.

I. Instructions for the Agency and IG Report

Each agency head shall transmit to the OMB Director a report that summarizes the results of annual IT security reviews of systems and programs, agency progress on correcting weaknesses[1] reflected in their POA&Ms, and the results of IGs independent evaluations. Additionally, the agency head shall send copies of complete IG independent evaluations. This report shall be based on work conducted during the FY03 reporting period only.

For national security programs and systems, FISMA includes the same program and review requirements as for non-national security programs and systems, but limits OMB's role to one of management and budget oversight. Thus, agency reporting to OMB in this area should be limited to providing within the report a separate section describing how the agency is implementing the requirements of FISMA for national security programs and systems.

The program description should include whether or the extent to which the management and internal oversight of an agency's national security programs and systems are being handled differently than the program for non-national security programs and systems and why. The description should also identify the number of independent evaluations conducted. Agencies must also develop POA&Ms (see Attachment C) for identifying and managing weaknesses in their national security programs and systems, but for obvious sensitivity reasons, they need not be fully integrated with POA&Ms for non-national security programs, nor should they be sent to OMB.

1 Unless specified as a material weakness, the term weakness refers to any and all IT security weaknesses. When the guidance refers to material weakness, the term material weakness will be used.

The agency report shall consist of two separate components. One is to be prepared by the IG2, characterizing the results of their independent evaluations and agency progress in implementing their POA&Ms. The other component is to be prepared by the CIO, working with program officials, reflecting the results of their annual system and program reviews and progress in implementing their POA&Ms.

These reports continue to be the primary basis of OMB's summary report to Congress. As such, please note that reporting performance against the provided measures is not optional. All agencies shall respond to each of the performance measures in the format provided. Agencies must provide empirical data in their report at a level of detail appropriate to support OMB's executive level review. The best illustration of this level of detail is that customarily found in IG and General Accounting Office (GAO) audit reports. Including many volumes of agency policies and instructions is not appropriate for an executive level review.

The report, consisting of both the IG and agency components, shall be submitted in the spreadsheet format provided. Annual reports under FISMA must now be sent to OMB and the Committees on Government Reform and Science of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, the authorization and appropriations committees for each individual agency of Congress, and GAO. Agencies may forward their report to the appropriate Congressional Committees and GAO after it has been reviewed by OMB and OMB has notified the agency. Copies of the IG's independent evaluations may be released to Congress any time following their submission to OMB.

Each agency head shall submit their report (both agency and IG components), and copies of the IG independent evaluations to OMB on September 22, 2003. Please note that this information should be sent to OMB following the directions in the cover memorandum to which these reporting instructions are attached.

Part II of this attachment provides additional information, in the form of Q&As, to agencies to assist them in implementing FISMA and OMB requirements.

Specific Instructions for the Agency Report

Responses to the questions below must be in the format provided. To assist agencies and oversight authorities in distinguishing between weak and strong performing agency components, each question below requires two responses, unless otherwise specified, an agency total and a breakdown by major agency component or bureau.

A. Overview of FISMA IT Security Reviews

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate.

---

2 Per FISMA, for each agency without an IG, the head of the agency shall engage an independent external auditor to perform the evaluation.

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.

Bureau Name	FY03 IT Security Spending ($ in thousnds)
Agency Total	

A.2.a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

Bureau Name	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Agency Total						
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes			No		
c. If yes, what methods are used? If no, please explain why.						
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes			No		
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes			No		
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.						

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.				
	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Agency Total				

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		

B. Responsibilities of Agency Head

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to the following questions:

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.	
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.	
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	

C. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.

a. Has the agency fully identified its national critical operations and assets?	Yes		No	
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes		No	
c. Has the agency fully identified its mission critical operations and assets?	Yes		No	
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes		No	
e. If yes, describe the steps the agency has taken as a result of the review.				
f. If no, please explain why.				

B.6. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).				
b. Total number of agency components or bureaus.				
c. Number of agency components with incident handling and response capability.				
d. Number of agency components that report to FedCIRC.				
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?				
f. What is the required average time to report to the agency and FedCIRC following an incident?				
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?				
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes		No	
i. If yes, how many active users does the agency have for this service?				
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes		No	
k. Do these configuration requirements address patching of security vulnerabilities?	Yes		No	

B.7. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.

Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement

C. Responsibilities of Agency Program Officials and Agency Chief Information Officers

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to identify and describe the performance of agency program officials and the agency CIO in fulfilling their IT security responsibilities.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total															

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N

II. Q&As for CIOs, Agency Program Officials, and IGs

A. Guidance for CIOs and Agency Program Officials

CIOs working with program officials must respond to all the questions in Part I. Responses must follow the prescribed format and should be based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their POA&Ms3, and any other work performed throughout the reporting period. Incomplete reporting against the provided performance measures will make the entire report incomplete and unacceptable.

Must agencies report at both an agency-wide level and by individual component?
Yes, agencies must provide an overall agency view of their security program, but most of the topic areas also require specific responses for each of the major components (e.g., bureaus or operating divisions). Thus, the agencies' and OMB's report can distinguish good performing components from poor performers and more accurately reflect the overall agency performance. For agencies with extensive field and regional offices, it is not necessary to report to OMB on the performance of each of the field offices. Rather, agencies should confirm that the agency-wide security program or the security program of the major component which operates the field offices is effectively overseeing and measuring field performance, that any weaknesses are included in the agency's POA&M, and that the office responsible for programs and systems are developing, implementing, and maintaining their POA&Ms.

When should program officials and CIOs provide the results of their reviews to their agency IG?
Program officials and CIOs should share the findings from program and system security reviews with their IG as they become available.

Do all agency systems have to be reviewed annually?
Yes. Senior agency program officials and CIOs must review all programs and systems at least annually. The purpose of the security program discussed in FISMA is to ensure the protection of the systems and data covered by the program, thus a review of each system is essential to determine the program's effectiveness. Only the depth and breadth of such system reviews are flexible.

What level of review is required for an individual system?
Program officials and CIOs are responsible for reviewing the security of all programs and systems under their respective control. Such reviews are not adequate without a review of all systems supporting such programs. Clearly, the necessary depth and breadth of an annual system review depends on several factors such as: 1) the potential risk and magnitude of harm

---

3 Agency POA&Ms must reflect all known security weaknesses within an agency including its components or bureaus and shall be used by the agency, major components and program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.

to the system or data; 2) the relative comprehensiveness of last year's review; and 3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation (consistent with NIST or national security guidance), this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented within the agency. The salient point is that an effective security program demands comprehensive and continuous understanding of program and system weaknesses. At a minimum, agency program officials and CIOs must take into account the three criteria listed above in determining the appropriate level of review for their systems with the understanding that all systems must be reviewed annually. IGs may report on the adequacy of such reviews.

What methodology must agencies use to review systems?
Agencies should use NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems" to conduct their annual reviews. Another guide may be used if the agency and the IG confirm in their report, that any agency developed methodology captures all elements of the NIST guide.

What performance measures must agencies use?
OMB has provided performance measures for a number of the questions. Some of the questions have specific management performance measures against which agencies (including major components) must measure their actual level of performance. In many cases, completing the performance measures is an adequate response to the question. However, agencies may provide a narrative response, if necessary, in addition to the numerical response to the performance measures. The OMB provided performance measures represent a minimum required response and must be completed. If an agency has developed additional performance measures, they may be reported as well.

What reporting is required for national security programs and systems?
FISMA requires that all programs, including national security programs, be reviewed every year. Reporting to OMB in this area should be limited to describing within the report how the agency is implementing the requirements of FISMA for national security programs and systems. The program description should include whether or the extent to which the management and internal oversight of an agency's national security programs and systems are being handled differently than the program for non-national security programs and systems and why. The description should also identify the number of independent evaluations conducted.

To assist oversight by appropriate national security authorities, it is important to specify where practicable which portion of the agency report pertains to national security systems.

What constitutes a significant deficiency?
OMB interprets a significant deficiency to include failure to meet FISMA's delineated requirements for an agency security program including the failure to substantially comply with related policies, guidance, and standards (e.g., this implementing guidance, OMB reporting guidance, OMB policy circulars and memoranda, and NIST guidelines and standards).

In the IT security program context, a significant deficiency would include the failure to perform adequate annual program and system reviews, failure to maintain comprehensive POA&Ms, and failure to adequately train agency employees and contractors.

In the context of individual systems, OMB Circular A-130 Appendix III provides three specific examples of a significant deficiency, each of which must be reported as such – the failure to assign responsibility for security of the system or application, the lack of system security plan, and the absence of authorization to process (certification and accreditation). Depending on the level of risk and magnitude of harm to the system, other weaknesses may also rise to the level of a significant deficiency.

B. Guidance for Agency Inspectors General

FISMA directs IGs or their designee, to perform an annual independent evaluation of the information security program and practices of the agency including a review of an appropriate subset of agency systems. In this regard, FISMA does not limit the subset to financial systems. To ensure a complete picture of an agency program, IGs should evaluate a representative sampling of all types of agency systems. FISMA also permits IGs to use the results of any other review in performing their work which occurred during the FY03 reporting period.

IGs should respond to all questions in Part I with the exception of question A.1. IGs should use the performance measures to assist in evaluating agency officials' performance. IG responses should be based on the results of the independent evaluations, including agency progress in implementing and maintaining their POA&Ms, and any other work performed throughout the reporting period (e.g., financial statement audits).

Additionally, IGs are asked this year to assess against specific criteria whether the agency has developed, implemented, and is managing an agency-wide POA&M process. The IG's assessment in this area is critical. Effective remediation of IT security weaknesses is essential to achieving a mature and sound IT security program and securing our information and systems. The IG's assessment of the agency's POA&M process is also instrumental to agency's ability to get to green under the Expanding E-Government Scorecard of the President's Management Agenda. Agencies must meet three criteria to get to green for security under the E-Gov scorecard, one of which is the positive assessment by their IG that an agency-wide POA&M process has been implemented.

Should IGs audit an agency's IT security program?
Within the context of FISMA an audit is not contemplated. FISMA directs IGs or their designee, to perform an annual independent evaluation. By requiring an evaluation but not an audit, FISMA intended to provide IGs some flexibility as to the degree of cooperation with CIOs and program officials as well as with the rigor of their review. OMB encourages IGs to take advantage of that flexibility while ensuring the appropriate degree of accuracy, independence, and objectivity.

Should IGs review the agency CIO/program official report to OMB to develop their independent evaluation?
Not as the exclusive input for their review, no. Neither FISMA nor OMB guidance requires such a review nor does such a review constitute meeting FISMA's requirements for IGs. Inasmuch as IGs, CIOs, and program officials should work together throughout the year to ensure the development and maintenance of a comprehensive POA&M and collaborate on preparing the report to OMB, a separate review of the CIO/program officials' report should not be necessary. Regardless of the approach taken, IGs should not rely solely on a review of the CIO/program officials' report as fulfilling their requirements under FISMA nor should any such IG review result in artificial deadlines that restrict the amount of time allotted for comprehensive agency program and system reviews by CIOs and program officials.

Should IGs validate agency responses to the IT security performance measures?
No. OMB is not requesting IGs to validate agency responses to the performance measures. Rather, as part of IGs' independent evaluations of a subset of agency systems, IGs should assess the reliability of the data for those systems they evaluate.

ATTACHMENT C

Attachment C consists of three parts:

- Part I – which provides guidance on POA&Ms, requirements of an agency-wide POA&M process, guidance on submitting POA&Ms and their quarterly updates, and guidance on reporting on performance measures.
- Part II – which provides examples of program and system-level POA&Ms.
- Part III – which provides a series of questions and answers to further assist agencies and IGs in developing, implementing, and reporting on POA&Ms.

I. Updated Guidance on Quarterly Reporting – Agency Plans of Action and Milestones and Performance Measures

A. Agency POA&Ms

OMB policy requires agencies to prepare and submit POA&Ms for all programs and systems where an IT security weakness has been found. The guidance directs CIOs and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets). Additionally, program officials shall regularly (at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

POA&M Requirements

Agency POA&Ms must:

1. Be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.
2. Include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool.
3. Be shared with the agency IG to ensure independent verification and validation.
4. Follow the format detailed in the examples under Part II of this attachment.
5. Be submitted twice a year to OMB (October 1, 2003 and March 15, 2004).

Quarterly Updates on POA&M Implementation

Agencies must provide on a quarterly basis in the table format below an update on their IT security remediation efforts. The first FY03 quarterly update is due on October 1, 2003. Remaining quarterly updates are due on December 15, 2003, March 15, 2004, and June 15, 2004. The quarterly updates must be reported in the format below.

Quarterly POA&M Updated Information	Programs	Systems
a. Total number of weaknesses identified at the start of the quarter.		
b. Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter.		
c. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled.		
d. Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.		
e. Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).		

Assisting Congressional Oversight

OMB's guidance to agencies on their POA&Ms was designed to: 1) first and foremost be a management tool to assist agencies in closing their security performance gaps; 2) secondly, assist IGs in their evaluation work of agency security performance; and 3) lastly, assist OMB with our oversight responsibilities. As a result and by design, these plans contain predecisional budget information. Per longstanding Executive Branch policy and practice, OMB and the agencies have a responsibility to maintain the confidentiality of predecisional, deliberative budget related information. OMB has addressed this issue in the guidance last year, which we continue in the FY03 FISMA guidance, to enable agencies to release information from their POA&Ms to Congress so that it may carry out its oversight role, while preserving the confidentiality of the Executive Branch's pre-decisional discussions.

Additionally, copies of these quarterly updates have also been requested by the House Government Reform's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. Agencies shall send their updates to the Subcommittee after review and notification by OMB.

B. Quarterly Reporting on Performance Measures

Beginning with the December 15, 2003, quarterly update, agencies will also provide a quarterly update on their performance against a subset of the performance measures in OMB reporting instructions. This update should be submitted with the quarterly POA&M updates and must follow the format below.

Quarterly IT Security Performance Measures Update															
Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total															

C. Quarterly IT Security Reporting and the President's Management Agenda Scorecard

Both the POA&Ms and IT security performance measures quarterly updates enable the agency and OMB to monitor agency remediation efforts to more accurately identify progress and problems. Additionally, these updates are also used to assess agency IT security status and progress under the Expanding E-Government Scorecard under the President's Management Agenda.

IT security is one of a number of critical components agencies must meet to get to green (or yellow) for the E-Gov Scorecard. If the IT security criteria are not successfully met, agencies will not be able to move forward to yellow or green, regardless of their performance against other E-Gov criteria. These quarterly updates from agencies directly inform the quarterly scorecard assessment.

To get to green for the IT security component of the E-Gov Scorecard agencies must:

- Demonstrate consistent progress in remediating IT security weaknesses through their POA&Ms;
- Have IG verify that there is a Department-wide IT security POA&M process; and
- Have 90% of operational IT systems properly secured (e.g., certified and accredited), including mission-critical systems.

To get to yellow for the IT security component of the E-Gov Scorecard agencies must:

- Demonstrate consistent progress in remediating IT security weaknesses through their POA&M updates and either:
  - Have IG verify that there is a Department-wide IT security POA&M process; **OR**
  - Have 80% of operational IT systems properly secured (e.g., certified and accredited).

In the instance where an IG finds through their FY03 FISMA evaluation that the agency does not have an agency-wide IT security POA&M process that meets OMB criteria, OMB will work with the agency and IG to ensure that after the agency has addressed the weaknesses identified by the IG, a timely follow-on review by the IG occurs. This step will avoid unnecessary delays in preventing an agency from moving forward on their E-Gov Scorecard.

II. POA&M Instructions

The following instructions explain how the POA&M should be completed. Attached is one example POA&M for a program and one for a system. Each illustrates the appropriate level of detail required. Once an agency has completed the initial POA&M, no changes should be made to the data in columns 1, 4, 5, and 7. The heading of each POA&M must include the unique project identifier from the exhibits 300 and 53, where applicable.[4]

Column 1 -- Type of weakness. Describe weaknesses identified by the annual program review, IG independent evaluation or any other work done by or on behalf of the agency. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity. Where more than one weakness has been identified, agencies should number each individual weakness as shown in the examples.

Column 2 -- Identity of the office or organization that the agency head will hold responsible for resolving the weakness.

Column 3 -- Estimated funding resources required to resolve the weakness. Include the anticipated source of funding (i.e., within the system or as a part of a cross-cutting security infrastructure program). Include whether a reallocation of base resources or a request for new funding is anticipated. This column should also identify other, non-funding, obstacles and challenges to resolving the weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc).

Column 4 -- Scheduled completion date for resolving the weakness. Please note that the initial date entered should not be changed. If a weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 8, "Status."

Column 5 -- Key milestones with completion dates. A milestone will identify specific requirements to correct an identified weakness. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the Column 6, "Changes to Milestones."

Column 6 -- Milestone changes. This column would include new completion dates for the particular milestone. See example.

Column 7 -- The agency should identify the source (e.g., program review, IG audit, GAO

[4]OMB Circular A-11 requires that agencies develop and submit to OMB business cases (exhibit 300) for major IT projects. Additionally, each agency submits an exhibit 53, a list of both major and non-major IT systems. The agency assigns a unique identifier to each system and includes it with these exhibits.

audit, etc.) of the weakness. Weaknesses that have been identified as a material weakness, significant deficiency, or other reportable condition in the latest agency Inspector General audit under other applicable law (e.g., financial system audit under the Financial Management Integrity Act, etc). If yes is reported, also identify and cite the language from the pertinent audit report.

Column 8 -- Status. The agency should use one of the following terms to report status of corrective actions: Ongoing or completed. "Completed" should be used only when a weakness has been fully resolved and the corrective action has been tested. Include the date of completion. See example.

Sample Agency or Program-level Plan of Action and Milestones
Agency, Component, and Program Name -- Department of Good Works, Major Service Administration

Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status
1-- No program-level security program/plan	Program office and agency CIO	None	3/1/02	Draft plan prepared and circulated for user input -- 11/30/01		Yes--5/17/01 report	Ongoing
				Comments reviewed, final draft to Administrator for approval and publication -- 3/1/02			
2 -- No documented program to report external security incidents to law enforcement and GSA	Program office and agency CIO	None	10/31/01	Consult with agency IG, FBI/NIPC, and GSA - 10/15/01			Completed
				Procedures published, employees trained 10/30/01			
3 -- No documentation for data sensitivity levels -- thus cannot document acceptable risk and security needs	Program office and agency CIO	$25K	1/30/02	Review enterprise architecture (process and data layers) to define and categorize data type and sensitivity -- 12/1/01			Ongoing
				Identify acceptable risk for each level, identify protection needs, document, publish, and implement -- 1/30/02			
4 -- Security not integrated w/capital planning. Not shown in exhibits 300 & 53	Agency CIO	Estimated $15K	1/30/02	Review and update all program exhibits 300 & 53			Ongoing

System-level Security Plan of Action and Milestones

Cite unique project ID and name shown on exhibit 300 and security costs from exhibit 53. If no 300 or 53 cite name only:

Project ID = Project name = Security costs =

Weaknesses	**POC**	**Resources Required**	**Scheduled Completion Date**	**Milestones with Completion Dates**	**Milestone Changes**	**Identified in CFO Audit or other review?**	**Status**
1 -- Password controls improperly configured and not tested	Program office	None	10/1/01	Reconfigure and test password controls -- 10/1/01		Yes	Completed
2 -- Security plan is out of date, more than one year since last update despite new interconnections	Program office	None	11/30/01	Update plan and obtain independent review -- 11/30/01		No	Ongoing
3 -- No written management authorization prior to system operations	Program office & Agency CIO	None	12/30/01	Complete certification and accreditation procedures per up-to-date security plan and NIST guidance. Obtain written auth -- 12/15/01		Yes	Ongoing
4 -- System is contractor operated and contract does not include FAR security and privacy clause nor are contractor practices evaluated by agency	Program office, contracting officer, and agency CIO	None	1/30/02	Identify specific security requirements, including for contractor personnel, and revise contract accordingly -- 1/30/02		No	Ongoing
5 -- System vulnerabilities have not been periodically tested as specified in OMB policy and Security Act	Program office and agency CIO	$50K	1/15/02	Arrange for system vulnerability testing -- 10/15/01		Yes	Ongoing
				Identify from test report, additional required security controls -- 11/15/01			
				Implement and test new security controls and schedule retest -- 1/15/02			
6 -- Life cycle system costs not incorporated into system funding	Program office and agency CIO	None	10/30/01	Identify costs. Update Exh. 300 & 53. Reallocate funds from lower system priorities -- 10/30/01			

III. Q&As on POA&Ms and Quarterly Updates

What is a POA&M?
A plan of action and milestones (POA&M) is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

How many POA&Ms should an agency prepare?
An agency should develop a separate POA&M for every program and system for which weaknesses5 were identified in the FISMA reports, as well as those discovered during other reviews including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. Thus, the POA&Ms should either reflect consolidation with, or be accompanied by, other agency plans to correct security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments.

Who in the agency is responsible for developing a POA&M?
Agency program officials must develop, implement, and manage corrective action plans for all systems that support their operations and assets. CIOs must develop, implement, and manage corrective action plans for all programs and systems they operate and control.

Who uses the POA&M?
These plans are designed to be used largely by: (1) CIOs, program officials, and other appropriate agency employees to track progress of corrective actions; (2) IGs to perform follow-up work with agencies; and (3) OMB to assist in its oversight responsibilities and to inform the budget process.

How is the POA&M tied to the budget process?
To promote greater attention to security as a fundamental management priority, OMB integrated IT security into the capital planning and budget process. This integration is already producing tangible benefits by promoting security that comports with the agency's enterprise architecture, supports business operations, and is funded within each information system over its life-cycle. To further assist in this integration, the POA&Ms and annual security reports must be cross-referenced to the budget materials sent to OMB in the fall including exhibits 300 and 53.

Specifically, for each POA&M that relates to a project (including systems) for which a capital asset plan and justification[6] (exhibit 300) was submitted or was a part of the exhibit 53, the

5 The term weakness refers to any and all weaknesses, not just material weaknesses.
[6]OMB Circular A-11 requires that agencies develop capital asset plans for all capital asset acquisition projects and report to OMB, via an exhibit 300, those plans for all major acquisitions. For information technology projects, plans for major systems must be reported

unique project identifier must be reflected on the POA&M. This identifier will provide the link to agency budget materials.

On all POA&Ms which reflect estimated resource needs for correcting reported weaknesses, agencies must specify whether funds will come from a reallocation of base resources or a request for new funding. While the POA&Ms will not be used as agency funding requests by OMB, a brief rationale should be provided when a request for new funding is contemplated.

Are there special considerations for POA&Ms for national security systems or DOD mission critical systems?
Yes. Due to their special sensitivity and the unique way they are addressed in FISMA, reporting weaknesses in national security systems as well as certain systems under the control of the Department of Defense and Intelligence Community is being addressed differently than for other systems. Although we certainly suggest that agencies document corrective plans of action for their own use, we are not prescribing a particular format. Prior to reporting such corrective action plans to OMB, we request that you consult with us so that we can make appropriate arrangements as to level of detail and sensitivity of what you should report. We have made special arrangements with the Department of Defense and could adapt that procedure for the use of other agencies in reporting on national security systems.

What format should an agency use to create a POA&M?
Agencies must use the attached spreadsheet-type format for their POA&Ms. At a minimum, agency POA&Ms must contain the information found on the attached spreadsheet. Each program and system where a weakness was identified should have its own POA&M. Agencies may submit their POA&Ms to OMB via email or on diskette as a Microsoft Excel spreadsheet.

Should quarterly IT security reports be sent to the OMB Director from the agency head?
No. Quarterly updates may be emailed to OMB by the agency CIO.

May agencies release their POA&Ms outside of OMB?
To maximize the usefulness of these plans, OMB intentionally and specifically tied the plans to the budget process. This assists both the agencies and OMB in determining and prioritizing budget decisions. As a result and by design, these plans contain predecisional budget information. Per longstanding Executive Branch policy and practice, OMB and the agencies have a responsibility to maintain the confidentiality of the deliberative discussions that led to the President's budget decisions.

Congress clearly has a need for information about an agency's information security activities and FISMA compliance in order to carry out its oversight role. Therefore agencies may release to Congress, as requested, the following information (as described under section II, POA&M Instructions) from their POA&Ms: 1) type of weakness as reported under column 1;

---

to OMB. Agencies assign a unique identifier to each system and apply it to the exhibit 300 and 53.

2) key milestones as reported under column 5; 3) any milestone changes as reported under column 6; 4) source of identification of the weakness as reported under column 7; and 5) the status of the weakness as reported under column 8. This will enable agencies to release information from their POA&Ms to Congress so that it may carry out its oversight role, while preserving the confidentiality of the Executive Branch's pre-decisional budget discussions.

What level of detail and sensitivity should the POA&Ms include?
Detailed descriptions of specific weaknesses are not necessary, but sufficient data is necessary to permit oversight and tracking. For example, to the maximum extent practicable agencies should use the types of descriptions commonly found in reports of the GAO and IGs such as "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not been performed prior to system access," "physical access controls are insufficient," etc. Where it is necessary to provide more detailed data, the POA&M should note the fact of its special sensitivity.

What security precautions is OMB taking to adequately protect the POA&Ms?
As with all sensitive information within OMB, access to POA&Ms (particularly the collection of all POA&Ms) will be limited to those OMB officials and staff that have an explicit business purpose for their use.

ATTACHMENT D

Definitions of Key Words Referenced in OMB Guidance

Adequate Security (defined in OMB Circular A-130, Appendix III, (A)(2)(a))
Security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(c))
A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

General Support System or System (defined in OMB Circular A-130, (A)(2)(c))
An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

Information Security (defined by FISMA, section 3542(b)(1)(A-C)) Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

Information Technology (defined by the Clinger Cohen Act of 1996, sections 5002, 5141 and 5142)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes

computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Major Application (defined in OMB Circular A-130, (A)(2)(d))
An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Information System (defined in OMB Circular A-11, section 300)
A system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should also be evaluated against these criteria. Your agency Capital Planning and Investment Control Process may also define a "major system or project." All major systems or projects must be reported on exhibit 53. In addition, a "major" IT system is one reported on your "Capital Asset Plan and Business Case," exhibit 300. For the financial management mission area, "major" is any system that costs more than $500,000. Additionally, if the project or initiative directly supports the President's Management Agenda Items, then the project meets the criteria of "high executive visibility". Projects that are E-Government in nature or use e-business technologies must be identified as major projects regardless of the costs. If you are unsure about what systems to consider as "major," consult your agency budget officer or OMB representative. Systems not considered "major" are "small/other."

National Security System (defined in FISMA, section 3542 (b)(2)(A-B))
(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

(i) the function, operation, or use of which--
  (I) involves intelligence activities;
  (II) involves cryptologic activities related to national security;
  (III) involves command and control of military forces;
  (IV) involves equipment that is an integral part of a weapon or weapons system; or
  (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Plan of Action and Milestone (defined in OMB Memorandum 02-01)
A plan of action and milestones (POA&M), also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Program Review (defined by OMB guidance)
A program review, in the context of the work required under FISMA, is a review of the security status of an operational program and is not a security program itself. Each program must be reviewed annually to ensure: 1) risk assessments occur; 2) policies and procedures are risk-based and cost-effective and comply with existing laws and OMB policy; 3) security awareness training for all employees; 4) management testing and evaluation of the effectiveness of information security policies and procedures; 5) a process for remedial action; and 6) procedures for detecting, reporting, and responding to security incidents.

IT Security Costs (defined in FY05 OMB Circular A-11, section 53)
In determining information and IT security costs, Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the agency Inspector General. This includes the costs of:

- risk assessment
- security planning and policy
- certification and accreditation
- specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- authentication or cryptographic applications
- education, awareness, and training
- system reviews/evaluations (including security control testing and evaluation)
- oversight or compliance inspections
- development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
- contingency planning and testing
- physical and environmental controls for hardware and software
- auditing and monitoring
- computer security investigations and forensics

- reviews, inspections, audits and other evaluations performed on contractor facilities and operations.

2. Other than those costs included above, security costs must also include the products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

3. Many agencies operate networks, which provide some or all necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid "double-counting" agencies should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded therefore; if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the budget materials.

Security Plan (defined in OMB Circular A-130, Appendix III, (A)(3)(a)(2)(a-g))
For General Support Systems: Agencies shall implement and maintain a plan for adequate security of each general support system. The security plan shall be consistent with guidance issued by NIST. Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. System security plans must include: 1) a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system; 2) required training for all users to ensure security responsibilities are met; 3) personnel controls; 4) an incident response capability to share information concerning common vulnerabilities and threats; 5) continuity of support; 6) cost-effective technical security products and techniques; and 7) written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.

(defined in OMB Circular A-130, Appendix III, (A)(3)(b)(2)(a-g))
For Major Applications: Agencies shall implement and maintain a plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation.

Application security plans must include: 1) a set of rules concerning use of and behavior within the application; 2) specialized training for all individuals prior to access that is focused on their responsibilities and the application rules; 3) personnel security controls; 4) contingency planning; 5) appropriate security controls; 6) appropriate rules garnering the sharing of information from the application; and 7) public access controls where an agency's application promotes or permits public access.

Security Program (defined in OMB Circular A-130, Appendix III, (A)(3))
Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications: 1) assign responsibility for security; 2) have a security plan for all systems and major applications; 3) provide for the review of security controls; and 4) require authorization before processing.

Mr. PUTNAM. Thank you very much, Mr. Rush.

Our next witness is Ellis Merschoff. Mr. Merschoff is the Chief Information Officer for the Nuclear Regulatory Commission. Prior to serving as CIO, Mr. Merschoff was the Director of the Western Region for NRC. He had worked at NRC in various capacities since leaving the U.S. Navy in 1980. He was awarded the Presidential Distinguished Executive Award in 2000 and is a licensed professional engineer.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF ELLIS W. MERSCHOFF, CHIEF INFORMATION OFFICER, NUCLEAR REGULATORY COMMISSION

Mr. MERSCHOFF. Thank you, Mr. Chairman. I appreciate this opportunity to testify with regard to the activities of the U.S. Nuclear Regulatory Commission as they relate to the Federal Information Security Management Act.

The mission of the NRC is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure protection of public health and safety, to promote the common defense and security, and to protect the environment. Our headquarters is located in Rockville, MD, with regional offices located in Pennsylvania, Georgia, Illinois, and Texas. We have a technical training center located in Tennessee and resident inspector sites located at 70 nuclear power plants and fuel-cycle facilities around the country.

Although I have been the NRC's chief information officer for only 9 months, I have been with the NRC, as you stated, for 24 years. Of those 24 years, I was an NRC line manager for 18 years and served as a regional administrator for 6 years. I understand the operational and business needs of the NRC which allows me to contribute a perspective that enables the agency to effectively apply information technology to meet the business needs of the NRC while achieving the appropriate level of computer security for the agency.

As an agency, we have 4,000 interconnected computers that exchange approximately 100,000 e-mail messages and receive another 40,000 e-mail messages from the Internet every day. On a daily basis, we experience 500 attempts at reconnaissance of our systems, strip out 300 suspicious e-mail attachments, identify 100 attempts at denial-of-service attacks and isolate 10 virus occurrences.

The NRC has identified all major operational applications and support systems, each of which has been certified and accredited. Outstanding findings from risk assessments and other evaluations are entered into a tracking system, monitored and closed out when resolved. We review the security controls for each of these systems on an annual basis, using the self-assessment process provided by NIST and benefit from a strong working relationship with NRC's Office of the Inspector General.

The NRC emphasizes computer security awareness at all levels of the organization, from senior management to the individual employee and contractor. We require that each employee take an annual computer security awareness course which is available online to ensure accessibility at the employee's desktop.

The NRC holds an annual observance of International Computer Security Awareness Day, which has grown in participation over the past 10 years. In November 2003, close to half of our headquarter's population attended this event.

Like all Federal agencies, the NRC must contend with viruses and other malicious software. We download new virus definitions to all desktops and deploy relevant computer security patches as soon as testing ensures compatibility with the NRC's mission-related software. The NRC also utilizes announcements to notify staff about viruses, hoax, spam, and scams that might affect our staff. Ask Cyber Tiger is a regular column in the NRC's newsletter that seeks to answer employees' computer security questions. Our computer security staff created Cyber Tiger about 8 years ago to act as a spokesman and a logo character to convey our computer security messages.

The NRC is the only Federal agency with a comprehensive electronic document management system known as ADAMS for which the agency received the Archivist of the U.S. Achievement Award. ADAMS supports the creation, storage, retrieval and management of documents and records related to the NRC's core business functions. The system stores the agency's record copy in electronic form for efficient transfer to the National Archives and Records Administration. Users can search for, view the image of and print documents at their work stations regardless of geographic location. ADAMS software identifies and authenticates users and applies access controls to ensure that each document is viewed or modified only by appropriate individuals.

In summary, the NRC operates with offices across the Nation. We take computer security requirements very seriously and work toward a seamless integration of computer security in our day-to-day operations. The NRC's computer security challenges continue to evolve, and we continue to revise our program to address these new requirements. I appreciate the opportunity to appear before you today, and would be pleased to answer any questions you may have.

[The prepared statement of Mr. Merschoff follows:]

STATEMENT SUBMITTED

BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSION

TO THE

HOUSE GOVERNMENT REFORM COMMITTEE

SUBCOMMITTEE ON

TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS

AND THE CENSUS

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

"INFORMATION SECURITY IN THE FEDERAL GOVERNMENT: ONE YEAR INTO THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT"

SUBMITTED BY

MR. ELLIS W. MERSCHOFF

CHIEF INFORMATION OFFICER

SUBMITTED: MARCH 10, 2004

Mr. Chairman and Members of the Subcommittee, I want to thank you for this opportunity to testify with regard to the activities of the U.S. Nuclear Regulatory Commission (NRC), as they relate to the Federal Information Security Management Act (FISMA).

I will outline the NRC's responsibilities and the security issues that arise in meeting those responsibilities. I will then address the NRC's efforts to achieve FISMA compliance, and will highlight a few of the NRC's information technology (IT) systems.

The NRC was created as an independent regulatory agency in 1975, taking over the regulatory functions of the former Atomic Energy Commission. The mission of the NRC is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. The NRC's scope of responsibility includes regulation of commercial power plants; research, test, training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste.

Our headquarters is located in Rockville, Maryland, with regional offices located in Pennsylvania, Georgia, Illinois, and Texas. We also have a technical training center located in Tennessee, and we have resident inspector sites located at 70 nuclear plant and fuel cycle facilities around the country. For Fiscal Year 2004, the agency has a budget of $626 million and staffing of 3,059 full-time equivalents (FTE).

The NRC is headed by five Commissioners, who are appointed by the President and confirmed by the Senate to serve for five-year terms. The Executive Director for Operations (EDO), currently Dr. William D. Travers, carries out the policies and decisions of the Commission and oversees the agency's day-to-day operations. The Office of the Chief Information Officer (OCIO) is one of 15 headquarters and regional offices under the direct purview of the EDO.

The NRC recognizes the importance of providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides for development and maintenance of controls required to protect Federal information and information systems. The NRC has historically been focused on technical safety and security issues, and computer security is another facet of that overall concern. Congressional oversight and participation in Federal CIO groups have helped focus our computer security efforts to more effectively protect our computer systems. NRC has had a computer security program since 1980 and has adequately budgeted for the agency's information technology requirements. Our focus on computer security from project inception and throughout the project life cycle has enabled us to appropriately protect our computer systems.

As an agency, we have 4,000 interconnected computers that exchange approximately 100,000 email messages and receive another 40,000 email messages from the Internet every day. On a daily basis, we intercept an estimated 2,500 SPAM messages; experience 500 attempts at reconnaissance of our systems; strip out 300 suspicious email attachments; identify

100 attempts at denial-of-service attacks; and isolate 10 virus occurrences. In 2003, our monthly status reports to the Federal Computer Incident Response Center (FedCIRC) recounted more than 67,000 non-debilitating incidents.

The agency's external Web site comprises approximately 30,000 pages of information, which are visited an average of 350,000 times per month, by people in 175 countries, for a total of more than 3,000,000 pages viewed each month. Each year, we publish approximately 200 nuclear regulatory documents, edit about 15,000 pages, and respond to thousands of requests for information in the library and public document room.

As I mentioned, the NRC has had a formal computer security program in place since 1980. As the basis for that program, the NRC follows Federal guidance from the Office of Management and Budget (OMB), the National Security Agency (NSA), the General Accounting Office (GAO), and the National Institute of Standards and Technology (NIST). We also participate in a variety of related Federal organizations, including the Computer Security Program Managers' Forum, the Federal Information Systems Security Educators' Association, and the Committee on National Security Systems and its working groups. In addition, we interact with the Department of Homeland Security (DHS), FedCIRC, the Computer Emergency Response Team at Carnegie Mellon, the Computer Incident Advisory Capability under the Department of Energy, and other recognized computer security organizations with which we cooperatively monitor situations and share alerts, methods of dealing with problems, and related information.

The NRC considers the agency's overall computer security needs alongside other funding requests, and the computer security needs of projects are an integral part of our capital planning and investment control process. We carefully review IT-related budget submissions to ensure that computer security is appropriately included. OMB approved the NRC's major IT system Capital Asset Plans and Business Cases Exhibit 300s with overall high ratings of "4" and "5," with "5" being the best possible rating. This approval of every NRC Exhibit 300 verifies that the agency employs sound project management, presents a strong business case for each IT investment, and meets other administration priorities to define the cost, schedule, and performance goals for each investment. Scoring criteria include support for the President's Management Agenda, acquisition management, performance goals, security and privacy, performance-based management, and life-cycle costs.

The NRC's management directives define agency policy and are the foundation upon which all agency work is performed. The "Automated Information Systems Security Program Management Directive" defines the NRC's computer security policy and defines applicable organizational responsibilities and delegations of authority. This document also includes a handbook, which the agency uses to implement the policy, referring to other Federal guidance as appropriate.

The NRC has identified all major operational applications and general support systems, each of which has been certified and accredited. Outstanding findings from risk assessments, system security plans, security tests and evaluations, contingency plan tests, certifications, and accreditations are entered into a tracking system, monitored, and closed out when resolved.

We also review the security controls for each of these systems on an annual basis, using the self-assessment process provided by NIST. Each system must be recertified and accredited every three years or when a major modification is made to the system. New system developments or system modifications are reviewed for computer security issues at appropriate steps of the system development life cycle.

Another contributing factor to the success of the NRC computer security program is the strong working relationship between my staff and the staff of the Office of the Inspector General. Identified security issues are raised as they are found and discussed throughout the year in a collegial environment between the two offices to aid in issue resolution.

The NRC emphasizes computer security awareness at all levels of the organization, from senior management all the way down to the individual employee and contractor. The NRC requires that each employee take an annual computer security awareness course. The NRC has implemented this course as an online resource, to ensure accessibility at the employee's desktop. The online course presents topic area information, followed by a short quiz that enables the employee to determine how well he or she understood the information. Each employee can raise questions about the course and its content, make suggestions for improvement, request test modification throughout the course, and return to the course whenever he or she wishes to review particular segments. By the end of 2003, 98.5 percent of our employees, interns, and contractors had satisfactorily completed the course. We track completion by office and report to each office how many of the staff members have completed the course and how this number relates to the completion rate of other offices. This friendly competition has helped to improve participation.

The NRC also has an online course for Information Systems Security Officers (ISSOs), which 100 percent of our ISSOs have completed. While only 33 agency employees have significant IT security responsibilities and are required to take this course, an additional 255 employees and contractors have taken the ISSO course to further their knowledge and understanding of information security.

The OCIO also hosts an annual observance of International Computer Security Awareness Day, which has grown in participation over the past 10 years. In November 2003, close to half of our headquarters population attended this event. In hosting this annual event, we use different themes each year. The day begins with a special guest speaker, followed by vendor exhibits in our exhibit hall. Our computer security staff representatives distribute informative brochures, as well as anti-virus software for employees to use on their home machines (as permitted by our site license.) We also have a year-round rotating poster campaign in all elevator lobbies of the headquarters and regional facilities.

Like all Federal agencies, the NRC must contend with viruses and other malicious software, and we expeditiously deal with the presence of such software within the NRC's network through isolation and extermination. We automatically download virus definitions to all desktops to ensure the currency of the information, and we deploy relevant computer security patches as soon as testing ensures compatibility with the NRC's mission-related software. The NRC also utilizes Network Announcements (distributed via email and on our internal Web site) to notify staff about viruses, hoaxes, SPAM, and scams that might affect our staff while at work or even on their personal computers at home. Our computer security staff representatives also contribute articles to the NRC's monthly "News, Reviews, & Comments" newsletter. "Ask

CyberTyger" is a regular column in the newsletter that seeks to answer employees' computer security questions. Our computer security staff created CyberTyger about eight years ago to act as a spokesman and logo character to convey our computer security messages. This character has since been replicated and used by other Federal agencies.

It is also appropriate to note that the NRC is the only Federal agency with a comprehensive electronic document management system, known as the Agencywide Documents Access and Management System (ADAMS), for which the agency received the Archivist of the United States Award of Excellence. ADAMS supports the creation or capture, storage, retrieval, management, and dissemination of documents and records related to the NRC's core business functions, such as the licensing and regulatory oversight of nuclear reactor operations and other activities involving regulation of nuclear materials and nuclear waste. Access to these documents by both NRC staff and the public is essential to enable the NRC to carry out its mission. The system captures documents upon receipt or signature, and stores them electronically in a single central location or repository, rather than in numerous office-level locations, thereby ensuring the integrity and availability of the document collection. The system also allows for electronic distribution of incoming documents, thereby eliminating substantial paper duplication efforts and making documents more quickly available for review. Because ADAMS makes documents available in electronic form, the system improves efficiency by effectively facilitating the re-use of documents by agency staff. The system also stores the agency's record copy in electronic form for efficient transfer to the National Archives and Records Administration. In addition, users can search for, view the image of, and print documents at their workstations, regardless of geographic location. As a result, documents are

now available to the public in minutes rather than weeks, and can be viewed and downloaded at no charge.

ADAMS customers and stakeholders include all NRC staff and licensees; law firms; various public interest groups and professional organizations; medical offices and hospitals; schools, universities, and students; many local, State, and Federal government agencies; and other members of the public. Nonetheless, access to documents stored in ADAMS is contingent upon the nature of the document. Some documents are available to everyone, but others can be viewed only by those with the proper authorization. ADAMS software identifies and authenticates users and applies access controls to ensure that each document is viewed or modified only by appropriate individuals.

The NRC receives electronic copies of documents from agency stakeholders, including the public, through our Electronic Information Exchange (EIE) system. EIE provides the capability to securely receive material related to official agency business from NRC customers and other Federal agencies across the Internet. The EIE system uses public key infrastructure and digital signature technology to authenticate documents, validate the identity of the person submitting the information, encrypt submitted data for storage in the EIE database, and decrypt stored data during retrieval from the database. This supports voluntary electronic submission of documents by interested parties to official agency proceedings, including licensees under Title 10, Part 50, of the *Code of Federal Regulations* (10 CFR Part 50).

Coupled with EIE, the NRC's Licensing Support Network (LSN) portal is the mechanism by which the parties (and potential parties) to the future high-level waste repository licensing

adjudication are to make all relevant documentary material available. The LSN replaces the classic "discovery" document exchanges among parties with electronic access to discovery materials beginning prior to the docketing of a license application. The Web-based LSN portal (www.lsnnet.gov) connects each party's document collections on whatever hardware and software platform they choose, within general guidelines reflecting agreed upon standards and formats.

In summary, the NRC operates with offices across the Nation and interacts with the public in general informational, regulatory, and discovery interchanges. In each of these interchanges, we take the inherent computer security requirements very seriously and work toward a seamless integration of computer security in our day-to-day operations. The NRC's computer security challenges continue to evolve, and we continue to revise our computer security program to address these new requirements.

I appreciate the opportunity to appear before you today and I would be pleased to answer any questions you may have.

# # #

Mr. PUTNAM. Thank you very much, Mr. Merschoff.

Our fourth witness for the second panel is Kerry Weems. Mr. Weems is in his 23rd year of Federal employment, 21 of those being at the Department of Health and Human Services. In 1988, Mr. Weems left the Social Security Administration and began work for the budget office in the Office of the Secretary, Department of Health and Human Services. Since then, he has served in a variety of capacities ranging from senior analyst to branch chief and division director. In June 2002, he became Deputy Assistant Secretary for Budget and, since January 2003, has served as Acting Assistant Secretary for Budget, Technology, and Finance.

You are recognized for 5 minutes. Welcome to the subcommittee.

STATEMENT OF KERRY WEEMS, ACTING ASSISTANT SECRETARY FOR BUDGET, TECHNOLOGY AND FINANCE, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. WEEMS. Thank you, Mr. Chairman. It is a pleasure to be here. And thank you for inviting me today.

Today, I would like to describe to you the existing efforts HHS has undertaken to improve the security posture of our agency and to comply with Federal legislative and regulatory directives.

In its most recent FISMA report, HHS reported 222 systems, 13 programs and 77 contractor operations and facilities, all of which require information technology protection. I would first like to summarize the current state of information technology security within HHS and the actions underway to address identified weaknesses and improvements that are currently underway.

I am pleased to report that improvements are being made in the management of information security at HHS. We have built a solid foundation and policy and procedures for IT security operations and management, including a series of supporting guides to assist personnel throughout HHS in understanding and implementing security policies and guidance. These policies and guides form a common baseline for standard IT security throughout the Department, which our operating divisions can exceed if their business operations require stronger protections.

Updates were also made on previous policies to meet new guidance from OMB, specifically in the areas of privacy impact assessments, plan of actions and milestone, security performance, measures and metrics, security program reviews, and self assessments. Additional updates were made to address newly emerging technologies.

In addition to these efforts, the Secretary launched Secure One HHS, a comprehensive program that blends targeted IT security, technical support and assistance with managerial and operational changes designed to improve the methods and practices of all personnel with IT security responsibilities throughout the Department. This program provides the framework for adequately securing our information systems.

In fulfilling this initiative, HHS has demonstrated its commitment to protect the health and welfare of the American public. Key focus areas of Secure One HHS currently include critical infrastructure protection, system and program level security development, FISMA compliance, which includes numerous subcomponents

such as certification and accreditation and incorporation of plans of actions and milestones as a management tool.

In less than a year, HHS has made major progress in employing an extensive security program and increasing the level of security throughout HHS. We have taken decisive steps to remediate the weaknesses identified in the FISMA report, drafted new policies and issued new guidance considering integration of security into the system development lifecycle. We have linked IT security with capital budgeting by improving and integrating IT security elements into the exhibit 53 and 300 submissions required by OMB, and we have augmented our procedures for the IT investment review board to ensure that IT security is addressed before new investments are made. We have implemented a streamlined yet very intensive support structure that provides our operating division with automated tools that improve and centralize data collection and reporting of FISMA plans of action milestones.

HHS has also licensed an automated NIST self-assessment tool to standardize and facilitate the department-wide utilization of NIST guidance. These tools are supplemented by extensive support and monthly plan of action and milestone review meetings with the information security officer of each operating division.

HHS has also drafted guidance concerning security certification and accreditation and developed remediation plans for ensuring certification and accreditation of all appropriate systems.

CNA compliance has increased in the last 6 months and is well on its way to exceeding its goal of 90 percent by June 30th of this year. As of today, we have achieved nearly 60 percent with a goal of 70 percent for the end of this month.

For systems that have not completed CNA, each system has a specific remediation plan targeting their path toward certification. Recently, security remediation plans have been expanded to track privacy impact assessments as well as linkages between system security and capital planning relationships. The chief information security officer has conducted reviews of the training and awareness policies and practices currently in place and issued guidance regarding the management of mandatory annual user security-awareness training.

Last, HHS is developing a departmental security operations center that will significantly improve our incident response capabilities and institutionalize a more rigorous defense against malicious hackers and other threats.

Thank you. That ends my testimony.

[The prepared statement of Mr. Weems follows:]

TESTIMONY OF

KERRY WEEMS

ACTING ASSISTANT SECRETARY FOR

BUDGET, TECHNOLOGY AND FINANCE

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

MARCH 16, 2004

Thank you for inviting me here before you today. It is an honor to have the opportunity to work with the subcommittee as it leads the effort to increase the security posture of all departments and agencies throughout the Federal Government. As the US Government's principal agency for protection of the health of all Americans, HHS is charged with carrying out a wide range of diverse missions that touch the lives of all Americans. Today, I would like to describe for you the extensive efforts undertaken to improve the security posture at HHS and to comply with federal legislative priorities.

The HHS mission covers a wide spectrum of activities including medical and social science research, prevention of infectious diseases, food and drug safety, financial assistance, child support enforcement, health, substance abuse treatment and prevention, comprehensive health services for Native Americans, the eradication of child abuse and care for the elderly. HHS consists of twelve Operating Divisions (OPDIVs), including eight agencies in the U.S. Public Health Service and three Human Services agencies that manage more than 300 programs with diverse missions. In addition, HHS is the largest grant-making agency in the Federal Government, providing approximately 60,000 grants per year.

In an effort to increase the efficiency with which HHS provides services to the public, HHS has greatly expanded its reliance upon information technology (IT). In its most recent Federal Information Security Management Act (FISMA) submission, HHS reported 222 systems, 13 programs and 77 contractor operations and facilities, all of which require IT security protection. HHS recognizes that a clearly defined and comprehensive IT security strategy is essential to continue supporting the delivery of critical health, safety, and wellness services to the public, and to safeguarding the information entrusted to HHS by the public.

I would first like to summarize the current state of information security within the Department, the actions underway to address identified weaknesses, and the

improvements that we are putting in place to improve our overall IT security management.

I am pleased to report that continual improvements are being made in the management of information security at HHS. We have thoroughly analyzed the previous findings of this subcommittee, as well as the audits and analyses of other groups such as the OMB and the Office of the Inspector General, and have used these as a foundation for our IT Security Program Plan and our Five Year IT Security Strategic Plan.

Similarly, we have built a solid foundation in policy and procedures for IT security operations and management, including a series of supporting guides to assist personnel throughout HHS in understanding and implementing security policies and OMB guidance. These policies and guides provide a common baseline standard for IT security throughout the Department, which OPDIVs can exceed if their business operations require stronger protections. We have published final versions of the following guides:

- Baseline Security Requirements Guide
- Configuration Management Guide
- Certification and Accreditation Guide
- Web Security Guide
- Risk Assessment Guide
- HIPAA Compliance Guide
- IT Penetration Testing Guide
- Incident Response Planning Guide

Updates were also made on previous policies to meet new guidance from OMB, specifically in the areas of Privacy Impact Assessments (PIAs), Plan of Actions and Milestones (POA&M), security performance measures and metrics, security program reviews, self-assessments, system characterization, and resource categorization. Additional updates were made to address newly emergent technologies, such as Voice-

Over Internet Protocol, wireless communications and wireless LANs, malicious code, system-to-system interconnection, peer-to-peer software and multifunctional wireless devices.

HHS has taken decisive steps to remediate the weaknesses identified in the last FISMA report. We have drafted new policy and issued guidance concerning the integration of security into system development life cycles. We have linked IT security with capital budgeting by improving our integration of IT security elements into our Exhibit 53 and 300 submissions, and we have augmented procedures for our IT Investment Review Board to ensure that IT security is addressed before new investments are made. We have implemented a streamlined, yet very intensive support structure that provides our OPDIVs with automated tools that improve and centralize data collection and reporting of FISMA POA&Ms and OMB management and reporting requirements through the HHS Information Security Data Management (ISDM) tool. HHS has also licensed an automated National Institute for Standards and Technology (NIST) 800-26 Self-Assessment tool, DataCure, Inc.'s Security Self-Assessment Tool (SSAT), to standardize and facilitate the Department-wide utilization of this important NIST guidance. These tools are supplemented by extensive coaching support, and monthly POA&M review meetings with the Information Security Officer of each OPDIV.

HHS has also drafted guidance addressing security certification and accreditation, and developed remediation plans for ensuring certification and accreditation (C&A) of all appropriate systems. C&A compliance has increased by 32% in the last six months and is well on its way to exceeding the goal of 90% C&A compliance by June 30, 2004. For systems that have not completed C&A, each system has a specific remediation plan targeting their path towards certification in order to enforce accountability for compliance with FISMA. Recently, security remediation plans have been expanded to track privacy impact assessments (PIA), as well as linkages between system security and capital planning relationships. The Chief Information Security Officer (CISO) has conducted reviews of the training and awareness policies and practices currently in

place for each OPDIV, developed gap analyses between these policies, established requirements and best practices, and issued guidance regarding the management of mandatory annual user security awareness training. Lastly, HHS is developing a Departmental Security Operations Center (SOC) that will significantly improve our incident response capabilities and institutionalize a more rigorous defense against malicious hackers and other threats.

Specifically, HHS has established a system of IT security-specific effectiveness and efficiency metrics that are used to track our progress throughout the year, rather than just through quarterly snapshots of status. Examples of these metrics include the percentage or number of systems with incident prevention, protection, and response capabilities, and the number of HHS employees who completed security awareness training, to name but a few. Metrics are updated and reviewed as required by departmental policy. These metrics enable IT security to be incorporated into the existing management information frameworks within each OPDIV, and will better illustrate the progress that an OPDIV has made in addressing security weaknesses and managing its IT security program. HHS is continuing to expand and refine these metrics to adapt to operational and regulatory changes and to provide ever-increasing usefulness for HHS management oversight.

In addition to this effort, HHS created and launched "Secure One HHS," a comprehensive program that blends targeted IT security technical support and assistance with managerial and operational changes designed to improve the methods and practices of all personnel with IT security responsibilities throughout the Department. This program provides the framework for adequately securing our information systems as required by the FISMA and is thoroughly described later in my remarks. In fulfilling this initiative, HHS continues to demonstrate its commitment to protect the health and welfare of the American public.

Drivers Towards Increased Security

A number of legislative, internal and external factors have guided HHS forward toward an enterprise wide approach to security. These factors include the following:

- **Emerging role of HHS as a key organization in the area of Homeland Security** – Certain Homeland Security initiatives, such as first-responder programs for biological, chemical, and terrorism attacks, and other domestic emergencies rely heavily on HHS resources and capabilities for information. Should key security functions be compromised during a crisis, critical information and IT resources could be compromised, worsening the impact of any emergency.

- **Growing Impact of Security** – As IT resources play an increasingly important part in fulfilling our mission of "improving the health, safety, and well being of the American people," our mandate requires us to protect those resources from the ever-increasing incidents of denial of service (DoS) attacks, computer viruses, system intrusions, and other malicious IT attacks.

- **Office of the Inspector General (OIG) Audits and Reports** – The HHS OIG conducts annual evaluations of the Department's information systems to identify weaknesses and determine vulnerabilities. These audits help substantiate that ongoing security protections meet both Federal guidelines and established IT security best practices, and enable HHS and OPDIV management to prioritize needed security improvements.

- **Secretary Priorities** – HHS Secretary Tommy Thompson has publicly stated that IT security is one of his top priorities. His One HHS vision also has ramifications within IT security: from the need to enhance communication and collaboration across HHS, to the need to consolidate IT infrastructures and common administrative systems while maintaining an overarching IT security program.

- **HHS Enterprise Strategic Goals**: IT security is directly integrated into three of HHS' five Enterprise Strategic Goals:
  - Provide a secure and trusted IT environment.
  - Enhance the ability of the Nation's healthcare system to effectively respond to bioterrorism and other public health challenges.
  - Achieve excellence in IT management practices.

- **HHS Enterprise IT Strategic Plan –** The HHS Enterprise IT Strategic Plan for FY 2003-FY 2008 defines the Department's IT mission, vision, goals, initiatives and measures including the development of an HHS IT security program.

Progress

In response to the above drivers, HHS has developed a comprehensive program to satisfy mission critical IT requirements. Three of the largest initiatives undertaken by the Department in FY2003 demonstrate the ongoing efforts to continuously strengthen the HHS security posture:

- **Critical Infrastructure Protection Plan and Project Matrix**
- **Creation and launch of the "Secure One HHS" program**
- **Increased implementation of Managed Security Services**

These initiatives reflect the Department's dedication to the rapid and sustained improvement of the IT security of the HHS information systems and the data that these systems transmit, process and store.

Critical Infrastructure Protection

The primary purpose of the CIP effort is to strengthen the Department's overall security posture in compliance with Homeland Security Presidential Directive/HSPD-7, which requires that the Executive Branch assess the cyber vulnerabilities of the nation's critical infrastructures – information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of federal, state, and local governments. This requirement is clarified in National Plan for Information Systems Protection Version 1.0

which states, "[t]he initial necessary step in preparing a defense of critical information systems and computer networks is a thorough assessment of the potential critical infrastructure system assets, interdependencies, and vulnerabilities."

The Project Matrix effort is an objective evaluation process designed to assist departments and agencies in determining their nationally critical functions and supporting infrastructure. While many of the Federal Government's infrastructure assets support national security, economic security, and public health and safety, not all require intensive protection activities. Project Matrix is designed to identify critical functions, services, and infrastructures that may require additional protections, so that resources are applied effectively and efficiently. HHS has been a leader in implementing Project Matrix.

The Critical Infrastructure Protection (CIP) initiative is centrally managed by Office of Information Resource Management (OIRM) and requires close coordination with all OPDIV Chief Information Security Officers (CISO) and Information Systems Security Officers (ISSO). CIP activities include revalidation of Project Matrix Phase I findings, Project Matrix Phase II analysis for CIP assets, Certification and Accreditation for CIP assets, FISMA corrective actions for CIP assets and update of the HHS CIP Plan and Automated Information Systems Security Program Handbook.

HHS launched its first Project Matrix effort in 1999, completing Phase I in 2000. Later legislation changed the Project Matrix methodology from an asset focused evaluation to one centered on function, thereby requiring HHS to revisit its Phase I work. In October 2003, HHS completed its revised Phase I, (the identification of critical functions and services and the primary supporting cyber and physical assets,) and successfully updated the CIP Plan. HHS depends on approximately 900 assets (both cyber and physical) to conduct day-to-day operations. The Department, with the assistance of the

Department of Homeland Security, identified twenty-four nationally critical assets and thirty critical functions.

The Department has initiated Project Matrix Phase II, the interdependency analyses on the critical assets. An interdependency analysis, or value chain analysis, is conducted on each nationally critical function and service in order to identify infrastructure functions, linkages, dependencies, potential vulnerabilities, and points of failure that could impact availability, reliability, and security of the asset, thereby hindering its performance. By way of illustration, Phase II Value Chain analyses were completed for the following functions at FDA:

- Approving the marketing of biologic products to include blood, vaccines, tissue, allergenics and therapeutics;
- Providing health warning information regarding post-market drugs and biologic products.

We anticipate completing the interdependency analysis for both cyber and physical assets in 2006.

The steps in the Project Matrix methodology serve as the cornerstone of effective CIP management and provide important data to further infrastructure identification processes where assets are analyzed, dependencies recognized, vulnerabilities realized, threats identified and mitigation taken to prevent security weaknesses. One of the benefits of this effort is that it has improved the communication between HHS physical and cyber security operations as well as expanded the understanding of how cyber and physical assets interact. The information collected as part of this process is reported to OMB, as required by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" (A-130); Government Performance and Results Act (GPRA) Agency reports, and FISMA. Results of the analysis also provide information helpful to fulfilling reporting requirements, audits, risk mitigation and ensure efficient use of resources for security planning and budgeting.

Secure One HHS

Following Secretary Thompson's One HHS vision, we are implementing "Secure One HHS." The mission of Secure One HHS is to create an enterprise-wide secure and trusted IT environment in support of the overall HHS mission. Secure One HHS also identified program goals that define outcomes that support and enable the achievement of the Secure One mission. The Secure One HHS goals are the following:

Goal 1 - Improve the overall HHS IT security posture to protect confidentiality, integrity, and availability of IT resources.
Goal 2 - Ensure minimum security standards enterprise-wide, consistent with Federal guidelines and best practices.
Goal 3 - Support integration of IT security into HHS lines of business.
Goal 4 - Promote an environment where all employees' actions reflect the importance of IT security.

These goals provide the basis for development of the IT security program's action plans. The action plans provide detailed information on how the HHS IT security objectives will be executed, and are based on a results-oriented management approach. To ensure program success, Secure One HHS and the HHS CISO continuously track the progress of each action plan through a series of performance indicators.

As part of Secure One HHS, the Department has implemented a strong governance structure that clearly defines roles, responsibilities, and security expertise at both the Headquarters (HQ) and OPDIV levels. At the enterprise level, the Department CIO leads all Departmental IT efforts. At the OPDIV level, each OPDIV has its own CIO and IT security officer who is responsible for the IT security program within that OPDIV and responsible for compliance with the Secure One HHS Program.

This structure was selected because a "one size fits all approach" does not work for managing IT security within large and complex organizations like HHS. By managing

the program at the HQ level, HHS is establishing a consistent IT security foundation across the OPDIVs. However, by having OPDIVs control the implementation of HHS IT security policies, each OPDIV is empowered to incorporate or exceed standard HHS security controls consistent with their own unique operational risk levels and operating environments. For example, the HHS network connection security policy does not limit connections only to those from government owned equipment, whereas the FDA policy permits only FDA-owned equipment to connect to its internal network through its remote access solution. This policy helps FDA to ensure devices connecting to the FDA network are properly configured, and continuously maintained, and to adhere to the FDA security standards, thereby reducing the potential risk posed by poorly configured machines. This approach allows for the development of needed IT security standards while allowing the OPDIVs the flexibility and customization necessary to effectively protect their own systems, environments, and organizational missions.

Structurally, Secure One HHS is comprised of two distinct components: Program Development and Program Implementation. The Program Development component focuses on ensuring compliance with federal IT security mandates and regulations, as well as internal HHS goals and objectives (e.g., full certification and accreditation of Departmental systems). Additionally, the Program Development component determines the strategic direction of Secure One HHS. There are six focus areas supporting the Program Development component: Strategic Planning, Oversight and Evaluation (O&E), Performance Management, Policy and Guidance (P&G), Security Operations Center (SOC), and Security Architecture. The Program Implementation component provides targeted IT security implementation assistance to the OPDIVs. This implementation support helps enable the OPDIVs to achieve a consistent IT security baseline across the Department, while still allowing them to implement IT security measures commensurate with their own risk. Six focus areas compose the Program Implementation function: Service Design and Delivery (SD&D), Enterprise Integration (EI), Education and Awareness (E&A), Outreach, Privacy, and HHS Net.

Program Function	Description
Strategic Planning	*Develops the strategy of the maturing Secure One HHS and ensures that the strategy aligns with IT security priorities.*
Enterprise Integration	*Provides support and facilitates integration of IT security into enterprise initiatives.*
Policy and Guidance	*Coordinates and drafts policies and guidance in support of the maturing Secure One HHS.*
Oversight and Evaluation	*Reviews and evaluates Secure One HHS compliance with Federal Regulations, policy, and guidance.*
Education and Awareness	*Provides the data collection, analytical, instructional, and communications services required to assess current training initiatives, make recommendations, and produces and implements IT Security Education and Awareness products.*
Outreach	*Provides OPDIVs advisory services and implementation support, including FISMA surge support, and POA&M workshops, as part of a maturing Secure One HHS.*
Service Design and Delivery	*Develops and implements communications and service strategies to increase awareness, drive adoption, and build pride and trust in the Secure One HHS.*
Performance Management	*Provides process and technical infrastructure for quantifying all aspects of performance of the Secure One HHS, determining causes of problems, and empowering performance improvement within the context of mission priorities.*
Security Operations Center	*Provides the CISO with oversight and analytical capabilities as they relate to IT security incidents within the Department. Establishes incident reporting capability and ensures coordination of incident response with the OPDIVs. Also centralizes patch management services.*
Security Architecture	*Supports HHS EA vision by establishing enterprise-wide security standards and integrating security in the HHS lines of business and determines the requirements and standards for the target architecture.*
Privacy	*Develops and formalizes appropriate OCIO standards and management processes, resulting in the annual report of privacy compliance as required under Section 208 of the E-Government Act of 2002. This function is also responsible for collecting and monitoring privacy impact assessments at the department level.*
HHSnet Security Support	*Supports HHSnet development team to ensure appropriate IT security measures and safeguards are incorporated into the network infrastructure, thus increasing the IT security baseline across the Department.*

Key focus areas of the Secure One HHS Program currently include critical infrastructure protection (CIP), system and program level security development, and FISMA compliance, which includes numerous subcomponents such as C&A and incorporation of Plans of Action and Milestones (POA&M) as a management tool. Secure One HHS

enhances collaboration, communication and knowledge sharing within HHS and across the Federal Government. At the same time the enhancement for security to HHS assets provides safety and service to the American public through increased access to data and information.

The specific focus areas and activities of Secure One HHS have been developed to address the range of security practices and needs required by the diverse HHS enterprise and to support all IT security requirements. The focus areas give Secure One HHS the flexibility necessary to continue with its planned evolution. By targeting resources at specific IT security areas of focus, Secure One HHS is poised to continue to adapt to the changing nature of IT security threats and federal IT security requirements.

Ultimately, Secure One HHS contributes to the Department's maturing management programs and processes to improve the selection and evaluation of IT investments. HHS recognizes that all system security activities rely on an accurate and documented count of systems to ensure that sensitive information is protected. As such, establishing a comprehensive systems inventory has been a high priority in the Department. Our inventory efforts are closely interconnected with the HHS enterprise architecture efforts and remediation plans that are underway in order to benefit from synergies and consistencies across the enterprise.

At HHS, the relationship between the processes for IT system development and system inventory management and that of IT budgeting continues to expand. Justification of additional funds for existing projects as well as requests for new funding must account for security. One of the Secure One HHS standards is that all investments must be reviewed and approved by the CISO prior to submission to the IT Investment Review Board (ITIRB). If the project does not meet expectations in the area of security, the investment will not be allowed to proceed. Additionally, the ITIRB will not approve funding for projects without responsible risk management. HHS has also implemented a new capital planning and investment control (CPIC) policy and set of procedures to

reduce the risk of inadequate security protections as well as removing redundancies across investments enterprise-wide. We are also implementing a portfolio management tool that will enhance our visibility over IT investment projects and support the CPIC analysis. We believe the processes we have in place make capital planning and implementation at the program/system level more efficient, effective, and secure.

Managed Security Services

Managed Security Services includes 24/7 monitored Intrusion Detection Systems (IDS), vulnerability scanning, forensic analysis and related services. The Managed Security Services initiative has three key activities:

1. Establishing an incident response program which helps prevent, detect and manage information security incidents for HHS;
2. Providing a standardized process for identifying network vulnerabilities; and
3. Implementing a standardized process for responding to information security incidents in a timely manner.

The Managed Security Services activity includes 24/7 intrusion detection. Vulnerability scanning, security architecture, the installation of security prevention devices, and network monitoring services are other aspects of this Secure One HHS initiative. Over the past year, HHS has installed over three hundred additional intrusion detection devices and is in the process of installing another two hundred to provide an additional defense layer for the HHS network. The project also includes the addition of vulnerability scanning of HHS networks, servers and systems. The Managed Security Services initiative is a key component of the HHS Security Operations Center (SOC).

Integration of Security into Department wide initiatives

HHS is committed to ensuring enterprise wide security standards. Currently, three major Enterprise wide initiatives are underway, (UFMS, HHSnet, and the Small OPDIV

Infrastructure Consolidation,) all of which will require coordination and integration of high priority safeguards.

UFMS

Launched by Secretary Thompson as part of the One HHS initiative, the Unified Financial Management System (UFMS) directly supports the President's Management Agenda (PMA) for financial management reform by consolidating and improving internal controls and financial reporting for the Department.

UFMS has two major components -- a part to support CMS called the Healthcare Integrated General ledger Accounting System (HIGLAS), and a part to support the rest of the Department. The goal of the UFMS program is to have an integrated Department-wide financial system that consistently produces relevant, reliable and timely financial information to support decision-making and cost-effective business operations at all levels throughout the Department. Benefits include:

- Reducing the resources and infrastructure needed to perform financial operations;
- Reducing the number of information flows between the administrative and core financial systems;
- Streamlining both internal and external financial reporting, and enable consolidated HHS financial reporting; and
- Taking advantage of advanced technical capabilities.

From system inception, the HHS's enterprise wide UFMS has planned and provisioned to secure the system and protect its data. UFMS serves as a flagship for the Department for its thoroughness in proactively addressing security at all levels. Management, operational, and technical controls are being implemented, thus providing a robust protection hierarchy.

The Healthcare Integrated General ledger Accounting System (HIGLAS) will give CMS enhanced oversight of Medicare contractor accounting systems and will provide high quality, timely data for decision-making and performance measurement. The new system, which uses commercial-off-the-shelf software that has been certified by the Joint Financial Management Improvement Program, is an application solution that will reduce internal control weaknesses through the assignment of strict roles and responsibilities of all its users.

HHSnet

The Department of Health and Human Services (HHS) Office of Information Resource Management (OIRM) has initiated a department-wide effort to modernize and consolidate the HHS networking and computing environment to a common IT infrastructure with common administrative systems shared by all OPDIVs and Staff Divisions (STAFFDIVs). Consistent with the Secretary's One HHS vision, the effort calls for the consolidation of HHS Wide Area Networks (WANs) and the consolidation of multiple service providers to a single service provider and a shared network backbone for the HHS enterprise network. The resulting system is referred to as HHSnet.

While HHSnet is intended to facilitate collaboration and efficiencies of service among the organizations of HHS, the consolidated solution also targets the three primary principles of security: confidentiality, integrity and availability. Based on controls planed for the final solution, HHSnet participants will benefit from a heightened security stance that will not only offer more security for inter-department communications, but will establish redundancies and sharing capabilities to dramatically increase the availability of services, assets and data. By standardizing the security stance of the new system, HHSnet will achieve a level of trust amongst HHS entities that is currently unparalleled.

There are three phases associated with the implementation of HHSNet. Phase I, expected to be completed this April, focuses on establishing a common HHS network backbone that allows HHS data traffic to pass securely between OPDIVs on the Government managed network instead of using the internet for connectivity. The goal of Phase I is to consolidate network vendors for each OPDIV under a single set of security parameters and providing a more manageable security environment. This effort will reduce the total number of Internet pipes going into HHS and help us to better secure these access points.

Phase II focuses on the traffic and services shared between OPDIVs. The goal of Phase II is to establish the infrastructure and security necessary to facilitate collaboration among the OPDIVs. This phase establishes what can be easily referred to as a "business partners" network, and institutes a common level of trust between the OPDIVs, standardizing the manner in which traffic is routed and filtered between both enterprise services and OPDIV specific communications. HHS and OPDIV stakeholders are still considering the final design for adoption, but it will incorporate centralized incident monitoring and response and redundancy for disaster recovery purposes.

Phase III focuses on consolidating connections to the Internet. The goal of Phase III is to use centralized access to external resources while facilitating a standard set of security controls for inbound and outbound traffic. The final design is still under consideration, but will include a common firewall and intrusion detection solution to control inbound and outbound traffic.

OPDIV Infrastructure Consolidation

Small OPDIV Infrastructure Consolidation:

Prior to the implementation the HHS consolidation programs, OPDIVs relied on multiple helpdesks, call centers and network vendors to provide IT infrastructure support. One major consolidation effort that is greatly improving reliability, availability

and confidentiality of HHS data is the consolidation of IT Infrastructure of the small OPDIVs (AoA, ACF, AHRQ, OS, SAMSHA, OIG and PSC). The IT Service Center (ITSC) provides IT infrastructure support for these OPDIVs. Through this consolidation, HHS has reduced the number of IT infrastructure support FTE from 144 to 53. One support contract replaced eight existing support contracts. This will streamline trouble handling and security incident response. Service hours have been expanded for all locations; including 24x7 network monitoring and call center services allowing HHS to respond to network issues quickly, even during non-duty hours. A single Call Center has been established to accept and manage all service requests, giving the ITSC a broad picture of the health and welfare of the network environment. Plans to consolidate servers and network devices are being developed and will be implemented in the next 18 months. Software and network standards will be implemented during the same period. Through these measures the ITSC will be positioned to provide better monitoring, and support to our customers.

Large OPDIV consolidations

AS previously stated, prior to the implementation the HHS consolidation programs, OPDIVs relied on multiple point of IT infrastructure within an OPDIV. To give a few examples of the success of this effort:

During FY2003 National Institutes of Health (NIH) has:

- Consolidated 14 existing email services into one centrally managed service.
- Consolidated 25 existing IT Help Desks into one centrally managed service.
- Consolidated 16 wireless networks into one, improving interoperability and security.
- Consolidated Security: Reduced four internet access points to two (necessary for fail-over).

Centers for Disease Control (CDC) has been working on the enterprise consolidation of 6 specific infrastructure services in FY 2003.

- Completed email server consolidation in November 2003.
- Reduced remote access servers from 6 to 2 in September 30, 2003.
- Consolidated 16 helpdesks to one centrally managed service.
- Consolidated hosting services from 30 to 1 by establishment of a Mid Tier Data Center (MTDC) and hot site facility The MTDC initial operation began in July 2003. Network connectivity between hot site and MTDC was operational by September 30, 2003. Ten mission critical applications are operational in the MTDC with real-time data replication to the hot site and 4 more planned within 6 months. 165 servers and 33 Tera Bytes of data are managed under the MTDC.

Centers for Medicare and Medicaid Services (CMS) completed its IT consolidation in 2002. Lockheed Martin, under the Consolidated IT Infrastructure contract (CITIC), assumed responsibility for the various components of the CMS IT infrastructure: consolidation into a single integrated help desk, desktop services, voice communications, mainframe, mid-tier, and network services, and hardware/software maintenance.

Food and Drug Administration (FDA) established the Office of IT Shared Services in October 2003. As a result an RFP for a single source performance-based contract for IT infrastructure support was published on January 28, 2004. FDA has completely transitioned to HHSnet and in fact leads the implementation and design teams in that effort. FDA also appointed an Enterprise Architect that is aggressively moving forward with the establishment of and FDA wide Architecture in accordance with the HHS EA programs.

As with the ITSC and the small OPDIVs these consolidations will pay security dividends through better reporting measures, decreases in response time during a security event and providing a secure, stable platform to host and transport HHS data.

HHS Enterprise Architecture

HHS is currently developing an approach to integrate security within the HHS Enterprise Architecture. This approach is being designed to employ OMB's Federal Enterprise Architecture reference models, security standards and secure processes advanced within government and industry. In response to these challenges, HHS will integrate security into the HHS Enterprise Architecture focusing on lines of business rather than using a system centric approach. The approach has been based on the guidance of OMB and NIST security guidance to develop a blueprint for a business driven enterprise security architecture solution leveraging the federal enterprise.

This program is necessary to ensure the protection of information and information systems categorized as National Critical Infrastructure, National Security Information, HHS Mission Critical, and all other sensitive assets. Protection of these assets is required in accordance with Homeland Security Presidential Directive-7 (HSPD-7), Public Law 100-235 (Computer Security Act of 1987), OMB Circular A-130, Federal Information Security Management Act (FISMA), federal regulations, and Executive Branch directions.

HHS Enterprise Email System (HHS-EES)

The consolidation of multiple HHS email systems into a single department wide e-mail system will improve the overall security of communications within the Department. Currently, there are over 200 e-mail servers, each with unique security, disaster recovery, and continuity of operations issues. By consolidating, the Department can ensure that all 75,000 users will have the same high standard of anti-virus protection, uniformly controlled physical and electronic system access, and improved system availability during emergencies. Additionally, by moving email systems out of potential terrorist targets, such as the NIH or CDC, the overall threat to the security of the system is reduced.

OPDIV SPECIFIC ACCOMPLISHMENTS

Centers for Disease Control

The Centers for Disease Control plays a critical role in protecting the public from the most widespread, deadly and mysterious threats against our health. CDC serves as the national focus for public health surveillance, bioterrorism preparedness, and outbreak investigations. Because of its importance for both Health and Human Services and Homeland Security, as well as the fact that it is a high profile target for malicious hackers and terrorists, the CDC has an especially significant need to protect its critical IT resources and the extremely sensitive and important information contained within them.

In the context of carrying out its mission, the CDC collects individually identifiable health information used to identify, monitor, and respond to disease, death, and disability among populations. This data must be protected to preserve individual privacy and respect individual dignity while maintaining the quality and integrity of health data.

CDC remains committed to federal and state public health information security and privacy practices, and is vigilantly implementing IT security controls to protect both the health and the privacy of the American public. During FY2003, CDC implemented a digital certificate program within the public health arena that enables for the secure and protected transmission of sensitive and critical information between public health organizations, including HHS. Over 6000 certificates were issued to external partners supporting 28 public health surveillance efforts. In addition, a special "two-factor authentication" program was established that allowed over 9,700 staff and partners to access the internal CDC network securely from virtually anywhere in the world.

CDC has also implemented the Secure One HSS intrusion detection initiative and installed both network-based and host-based intrusion sensors on critical systems and instituted full around the clock intrusion monitoring. This effort has enabled CDC to

increase the efficiency and effectiveness of its counter-intrusion activities. These technical and operational improvements have been complimented by an mandatory internal training program aimed at educating CDC employees and partners about the importance of IT security and their roles in protecting the information and IT resources with which the CDC has been entrusted. The CDC is proud to report that 99.92% of all employees have completed the security awareness training.

National Institutes of Health

The National Institutes of Health (NIH) is the principal biomedical research agency of the Federal government. NIH seeks to expand fundamental knowledge about the nature and behavior of living systems and apply that knowledge for improving human health and reducing the burdens resulting from disease and disability. The NIH also supports biomedical and behavioral research domestically and abroad, conducts research in its own laboratories and clinics, trains researchers and promotes the acquisition and dissemination of medical knowledge.

Researchers collaborating from around the world to solve complex health problems require a computing environment that balances the need for open scientific collaboration against protection of data falling into the wrong hands. In 2003, NIH changed its open network architecture to a restricted and consolidated firewall architecture that preserved the communications and collaborations necessary for NIH research and operations, but also dramatically reduced the potential for successful network intrusions. In addition, multiple virus walls, (including file stripping techniques,) were employed to enhance security in depth. These key network components have not only protected NIH against last year's worms and viruses but continue to provide protection against the latest round of attacks and attempted infections.

The NIH has coupled these technical improvements with changes in management and operations. The NIH CIO chairs a management committee that provides senior

leadership and direction on the NIH-wide IT security program. The committee evaluates issues related to the security and privacy of NIH IT systems and data, including but not limited to: (1) uniform and prioritized policy and procedures for system security problem avoidance and response; (2) appropriate technological approaches; (3) external access; and (4) backup and disaster prevention and recovery.

Operationally, the NIH Computer Security Awareness and Training Program is a highly successful initiative. More than 98% of NIH employees have taken the training, which applies an award-wining, web-based training approach. National and international organizations, including universities and medical schools, continue to request the course for their own staff. NIH provides a wide portfolio of IT security classroom courses that include basic security awareness to highly advanced training for IT security professionals. Timely and informative articles are included in agency newsletters (e.g., the importance of maintaining up-to-date patches and antivirus software), and brochures and extensive guidance documents are available to staff. Institute/Center IT security personnel pursue the HHS-sponsored professional certification courses, as well as advanced technical training to ensure knowledgeable, well-trained staff supports the agency. Additional training is offered at the monthly ISSO meetings, which are open to all IT security staff.

Food and Drug Administration

The Food and Drug Administration (FDA) ensures the safety of foods and cosmetics and the safety and efficacy of pharmaceuticals, biological products and medical devices.

Recently, the FDA successfully designed and implemented a remote access solution to enable authorized users to securely access internal FDA resources from non-FDA locations. Designed to allow only government (FDA) owned devices to remotely access its IT resources, the FDA secure remote access solution employs best-of-breed security technologies to provide "two-factor" user authentication and multiple layers of other protections to safeguard potentially sensitive data (such as pharmaceutical patent or

safety information) while it is resident on the computer and in transit. In an environment where innovative pharmaceuticals are reviewed to ensure that safe and effective products reach the market in a timely way, secure remote access is paramount to ensuring protection of both the integrity and sensitivity of this proprietary data.

In addition to its remote access solution, the FDA has implemented a robust security architecture, applying a "defense-in-depth" approach to ensuring adequate protection for its confidential information resources and its heavily visited public website. The implementation and continued enhancement of this security architecture, which includes various firewall technologies, an intrusion detection and monitoring capability, multi-layered virus protection and a security-focused extranet design, enables the FDA to more securely fulfill its mission.

The FDA has also successfully developed and implemented an information security awareness program to ensure that all users of FDA information systems receive adequate security training to perform their duties while meeting the IT security obligations. This training has focused on the user's responsibilities in maintaining operational continuity, reducing IT security risks, and meeting Departmental and Federal Government IT security rules and regulations.

FISMA Compliance Update

Since many of the gains mentioned above were realized after the FY 2003 FISMA cycle was complete, the 2003 FISMA evaluation does not fully reflect the current state of the IT security and privacy protections currently in place or in development throughout the Department.

In less than a year, HHS has made major progress employing an extensive security program and increasing the level of system security throughout HHS. The underlying cause for most of the weaknesses raised by the IG in the FISMA 2003 report stemmed

from the lack of an effective information security management program structure. Secure One HHS was created to respond to these weaknesses, and improvements are already being made. While there is more work to be done, significant progress has been made in the managerial, technological, and operational levels throughout the Department. HHS has made great strides in certification and accreditation, system inventory, integration of security into capital planning, development of policies and programs, training, and incident response. C&A compliance has increased by 32% in the last six months and is well on its way to exceeding the goal of 90% C&A compliance by June 30, 2004. For systems that have not completed C&A, each system has a specific remediation plan targeting their path towards certification in order to enforce accountability for compliance with FISMA. Recently, security remediation plans have been expanded to track privacy impact assessments (PIA), as well as linkages between system security and capital planning relationships.

Essential to managing the Department's security program is a comprehensive understanding of the number and severity of existing weaknesses. As such, Secure One HHS has created an automated POA&M reporting tool and has conducted POA&M monthly meetings, process reviews, and workshops for OPDIV personnel. Quarterly performance measures have also been implemented in order to improve the tracking of POA&M progress. As a result of these efforts, POA&Ms are also now used as a fully integrated IT management tool that tracks the correction of IT security weaknesses over time and effectively validates funding requests for IT security. The POA&M effort has been pivotal to improving management oversight by allowing comparison of multiple data sources to verify and validate the data received from OPDIVs.

Next Steps

Because the IT threat environment is ever changing and federal requirements must be adjusted to respond to these threats, HHS recognizes that our security program must continually adapt. The Department remains unwavering in its commitment to

continually seek out ways to improve the development, implementation, monitoring, and oversight of IT security. The evolving nature of IT at HHS demands that increased attention be placed upon IT security and its integration into the larger business and program culture of the Department and its OPDIVs.

HHS is streamlining its IT security data collection and tracking process, increasing management oversight and awareness, and reducing the overall time and resources expended for IT security reporting. When fully implemented this effort will result in more accurate, timely, and consistent data for budgetary and planning purposes. However, the existence of automated tools is not enough; they must also be intuitive to the user and provide a broad spectrum of actionable information. Therefore, HHS is transforming its current IT security data collection process into a true performance measurement initiative. Each Secure One HHS goal and objective has performance measures that not only allow for measurement of program implementation, but are also used to verify and validate the effectiveness and efficiency of implemented security measures, as well as their impact upon HHS mission and business lines.

One of the fundamental reasons for the establishment of Secure One HHS is to support the OPDIVs in adapting HHS IT security practices and incorporating them into their unique lines of business. The Secure One HHS Communications Plan is designed to facilitate this vision by developing a process to capture attention, gain understanding, and ensure cooperation as HHS expands and integrates its IT security measures. In addition to the Secure One HHS Communications Plan, a stronger and broader IT security awareness program is being established to positively change and reinforce behavior consistent with HHS IT security policy. The IT security awareness training course, and IT security rules of behavior, focuses attention on computer and information security, creating sensitivity to threats and vulnerabilities, and reinforces the active application of recommended security practices. Together, the implementation of both the Secure One HHS Communications Plan and the IT Security

Awareness Plan provide the strategy for expanding stakeholder commitment to the IT security program and driving cultural change within the Department.

Conclusion

HHS has made significant progress in implementing a comprehensive IT security program. We recognize that a successful IT security strategy calls for the institutionalization of sound IT security practices that are essential for the safeguarding of the information entrusted to HHS by the citizens of this country. We remain committed to this goal as we continue to implement the Secure One HHS Program and HHS will continue to work to further improve and expand the capabilities of the HHS IT security program.

In closing, I would like to reemphasize that HHS has a long history of protecting information critical to the American public and is well aware of the critical importance of security. We continue to listen and learn, and, we continue to act to improve how we protect ourselves and preserve the public trust. We are doing our part to carry out Congress' will to safeguard our future – with confident commitment and determination.

Mr. PUTNAM. If you have a wrap-up statement, you are welcome to make it.

Mr. WEEMS. OK. I will be happy to do that.

We have made significant progress toward implementing an IT security program. We recognize that a program and a strategy call for the institutionalization of sound IT security practices that are essential for safeguarding information entrusted to HHS by the citizens of the country. We remain committed to this goal as we continue to implement the Secure One HHS program. Thank you.

Mr. PUTNAM. Thank you. I thank you for your sensitivity to the little red light. Some people just keep right on going.

Mr. WEEMS. Mr. Chairman, I have sat behind many secretaries who have had to watch the red light.

Mr. PUTNAM. It can be intimidating. When I was in the State legislature, I had to testify before my first subcommittee, and it freaked me out when I went yellow much less red.

Mr. Merschoff, you are the teacher's pet of the panel. Your agency received an A, so we are going to give you all the first questions and then sort of let you off the hook, I guess.

You know, relative to some of the other agencies and departments, the NRC is relatively small. How much of your success was determined by your size and how much of your success is scalable in that it could be easily replicated in a larger organization?

Mr. MERSCHOFF. I would say size is a function of the timeliness of accomplishment and not the accomplishment itself. We are a full scope agency. We develop new IT applications. The ADAMS that I discussed is the first in the Government in terms of an electronic records management system. We are developing another one for an electronic courtroom for the high-level waste hearing.

So what we do is difficult, but being smaller allows us to proceed at a pace that is easier to maintain than the large agencies. In terms of scalable, I believe it probably is.

Mr. PUTNAM. Now that you are on top, how institutional are your changes? I mean, do you foresee remaining an A virtually indefinitely? What types of changes do you have to make on an ongoing basis to continue to meet those top standards for your A rating?

Mr. MERSCHOFF. Well, as Lewis Carroll said in Alice Through the Looking Glass, you have to run really fast in this world to just stay where you are, or words to that effect. The bar is being raised continuously by OMB, so it will be harder this year to be an A than it was last year. We have areas to continue to work on, two that you have addressed already in terms of contingency plans and inventories are areas we have work to do in. So there is important work that remains to be done relative to our agency.

I have an outstanding staff, and I have the support of the senior management within the agency to maintain computer security, so I anticipate we will be able to meet the new challenges.

Mr. PUTNAM. How have you implemented the accountability within all of your managers and program directors? How is that effective, and how have you helped them make it, make information and security a priority of their everyday life?

Mr. MERSCHOFF. We have established the corporate level procedures that govern the IT systems, chief of which is the capital planning and investment control process. We have integrated security

into the development of new systems, so a business line can't develop a new system without the approval of the Office of the CIO, and embedded in that approval is working hand in hand with us with security. So we have confidence that each new security system we bring on line is robust in a security sense. And being a peer to the other business line managers, they seek our help, and we provide it in terms of current operating systems.

Mr. PUTNAM. Your background is not technical in nature as it relates to IT; you are an engineer, I believe. Do you think that has helped you in understanding the importance of this and sharing it with others? Do you think that you have more credibility with your peers as an engineer as opposed to being an IT specialist?

Mr. MERSCHOFF. I would take issue with my background not being technical. I'm an aerospace engineer and a mechanical engineer.

Mr. PUTNAM. Information technical.

Mr. MERSCHOFF. I'm not an IT professional. I believe that has helped a lot. What I believe agencies need at the CIO level is an executive that can hold people and programs accountable to achieve certain goals. Engineering as a discipline is one that IT in general can benefit from. Engineers look at redundancy and reliability and bring a rigorous, disciplined thought process to systems development that matches nicely with IT development and CPIC development.

So the direct answer to your question, in terms of credibility, I believe it helps a great deal. Having been a peer to the senior business line managers in the agency, there is a trust in the budgeting process and there is a trust in terms of the service delivery process that I think helps us progress.

Mr. PUTNAM. Thank you.

Mr. Rush, could you please elaborate on the additional financial reporting requirements that took priority and pushed FISMA into a secondary position that you referred to in your opening statement?

Mr. RUSH. Yes, sir. In fiscal year 2002, we were the first Cabinet-level agency at Treasury to accelerate our financial reports to the shortened deadline of November 15th. Under Secretary Paul O'Neill, much effort was expended to demonstrate that financial reports had to be timely to be useful to managers. As we approached 2003, it was clear to OMB that was an important goal for all of the CFO agencies. Thus, by late spring, early summer and immediately following the divestiture of a lot of our resources, I met with the assistant for management and we consulted with the Comptroller of the United States Linda Springer and made clear that we couldn't meet the accelerated deadline for 2003 and meet our other requirements given the resources that we had lost. We were clearly able to produce one of those jobs but not both of them by the deadlines.

So the decision was that the IRS, the Bureaus, the Treasury IG for tax administration and the Department would prepare their report and send it to OMB on time and that the IG work that my office does to bring FISMA to conclusion would be followed within 30 days of any successful accelerated financial statement report.

Now, those discussions went on for a couple of weeks, and as I indicated to you in my letter, when I distributed the report to you I apologized for the first time, we did not think to notify this subcommittee because we assumed that having coordinated with OMB that information might have been available. I regret that. That was my responsibly, and I am here to accept that responsibility.

But as between the two important jobs that we were facing as we went into the fall, it was clear that the accelerated financial report was the priority for Secretary John Snow and for the administration.

Mr. PUTNAM. Is contracting out an option? I assume it will be, based on your earlier remarks. Is it going to be your option in the future to contract out the preparation of the FISMA reports?

Mr. RUSH. It will have to be for the foreseeable future, because, again, we are not moving our resources up. The President's budget request for 2005 gives us a substantial plus up over 2004. It almost helps us recover from some of the divestiture. But the problem here is timing. As we found last summer as we faced the decision of financial statement reporting, FISMA reporting, if you can't make those decisions early enough in the audit cycle, you can't get a contract out there. Our problem was that we were going into this audit period anticipating using our own resources to do the work, and when we had this tradeoff decision, we found ourselves in the position where it was too late to bring a contractor in because you still have to supervise the contractor.

This year we're starting off with better understanding of our resources, we're going to do more contract work for—our financial reporting, and we intend to use a contractor for most of our FISMA work. We'll not do it for the national security systems that we report on to you and others as classified reports.

Mr. PUTNAM. You went from 165 to 62 staff in the IG's office?

Mr. RUSH. No, that's just the audit staff.

Mr. PUTNAM. Audit staff. Is that proportional to the amount of the department that was transferred to the Department of Homeland Security?

Mr. RUSH. Well, after a careful study of our audit program for the 3 years prior to divestiture, we identified a need to transfer somewhere between 30 and 35 percent of our staff to Homeland to accompany the work that was associated with the Customs Service, the Secret Service, the Federal Law Enforcement Training Center and that part of the Bureau of Alcohol, Tobacco and Firearms that went to the Justice Department. But for reasons still not clear to me, we were cut 70 percent rather than 35 percent and we've been playing catch-up.

That decision was made, and clearly people were trying to do the right thing to establish the Department of Homeland. And I don't doubt that the people that we contributed to that IG office over there have made a difference in the Department of Homeland Security, but we had to actually go out and pick up about 12 people for the financial statement audit cycle and detail them into our office to get that audit done. And we are struggling.

Mr. PUTNAM. The IRS and Bureau of Public Debt, those audits are conducted by you or by the GAO?

Mr. RUSH. The IRS is done entirely by GAO and part of the public debt is done by GAO. We rely on those reports to prepare the consolidated. We're responsible for the consolidated audit and the bureau-level audits and special audits.

As you know, Treasury right now has eight different stand-alone audits, everything from the gold and silver reserve to special accounts. The recovery in D.C. pushed the pension funds from D.C. into Treasury, so we have to manage an account from those funds and do a financial statement on the retirement for judges and teachers and police officers.

We do stand-alone audits for the Office of the Comptroller of the Currency, the supervisor of national banks; the Office of Thrift Supervision, the supervisor of the savings and loan industry. We do stand-alone audits for other entities including the Financial Management Service, the check writer and the cash manager for government.

Mr. PUTNAM. And I hear where you're coming from on the reasons for the delay.

At the end of the day, the score was a D, and I'm told probably with the input of the IG's report, had it been on time, would have remained an F, the same scores received in 2002.

In your testimony, you attribute a fair amount of that to the IRS. Could you elaborate on that?

Mr. RUSH. Well, the IRS is the largest bureau of Treasury. Treasury right now is about 115,000 116,000 people; 100,000 are in IRS.

IRS has gone through major systems modernization for the last 4 or 5 years and into the foreseeable future. Their inability to accurately identify the number of systems that they had really changes all the numbers for Treasury because of the miscount or undercount of systems and the failure to develop plans consistent with all of those systems.

But I do not want to make that solely an IRS problem. Treasury in every level, in every bureau, has very serious information security problems.

Mr. PUTNAM. Well, to your credit, you're very blunt and candid in your opening statement and your submitted testimony to that fact. And it is, considering the nature of Treasury and the information it handles and the privacy issues surrounding it, people are sensitive about what they pay in taxes and what they have, I would think that you would be on the short list of folks that we would really want to get it right. And so it is important that Treasury can prove.

Mr. Weems and Mr. Corts, both of you are responsible both for financial management and budget, as well as technology of your agencies, I believe; is that correct?

Mr. CORTS. That is correct.

Mr. PUTNAM. One of the most common complaints that we hear is that the components level of departments don't follow department-wide policy on information technology and don't feel compelled to do so.

Do you find the same resistance when you direct budget or fiscal policy for the Department? And why is there a lesser standard of

accountability or responsiveness on issues related to information technology? Mr. Weems and then Mr. Corts.

Mr. WEEMS. The hammer of the budget produces, usually, the quickest results; if nothing else, it quickly gets the attention of the component head and produces an appeal to the Secretary, to me, to somebody else, who then can have a reasonable discussion about it.

Many times, things in other areas seem a bit too esoteric to be able to have that kind of discussion. That's why we have undertaken in HHS to link these things together. Investments in our budget process that do not have proper security simply won't go forward, and the agency head or agency official will be in the posture of having to appeal, having to have a discussion, and also having to explain why they're trying to move an information and technology investment that does not have security sufficient to the standard.

Mr. PUTNAM. Mr. Corts.

Mr. CORTS. There's always a certain amount of push-back.

I think that the Department of Justice was really—the decentralization of the Department caused the bureaus, especially the large bureaus, to really take on kind of a persona of their own and perhaps push back in both budget and IT is stronger in those kinds of situations. But I believe, over the last couple of years, with the emphasis on unity as a department, we're seeing a great deal of lessening of that.

The CIO Council that operates within the Department and I occasionally will drop in on their meetings. There seems to be a good spirit there and a real desire to try to work together. The way that we're organized, it does allow the CIO to be very involved in the budget process, and I believe it is becoming well recognized throughout the Department that the CIO has a significant role with respect to budgetary issues.

So the point that Mr. Weems was making where the budget is such a readily identifiable hammer, if you can tie that to IT, I think you have an additional kind of hammer to use. So I believe that the role that the CIO is playing in budget decisions, the CIO's involvement in our management team, is giving the CIO additional strengths and a way to deal with this push-back issue.

Mr. PUTNAM. This is the 4th year in a row that Justice has had an F score. What are some things that you can identify as barriers to breaking into that D category or something better than 4 years of an F?

Mr. CORTS. Well, frankly, we had a lot of organizational problems, as I described in the testimony, not the least of which was a clear identification of who was in charge of IT security. Again, I came to the Department about 16 months ago, and quite frankly, I was quite surprised with what I found with regard to IT and IT security.

But I think that we're making big strides, and one of those issues was a clear identification of who was going to have IT security, because it had previously, in the Department, been kind of jerry-rigged, I guess somewhat split between the Department security officer and the CIO. And there was a lot of struggle over the issue of naming one single person the ultimate person responsible for it,

but we've crossed that bridge and that's really helping us to move forward; and very quickly on the heels of that, the appointment of a chief information security officer, a person who came with a lot of skill and background and is just really making giant strides for us in the last months, that aren't showing up on scorecards yet because the scoring took place before some of these things were happening.

This is a very dynamic thing for us, and it's on the move, and I think it is on the move in the right direction.

Mr. PUTNAM. I am glad to hear it is on the move now, and I hope that it stays true. I was on the Horn subcommittee and we've heard from a lot of folks about changes in personnel, changes in priority, changes in leadership, changes in policies; and we have to institutionalize something that will outlast you, that will outlast me and your attorney general and this President and everything else to get serious about this.

Mr. Weems, your testimony indicated a number of excellent sounding initiatives, secure one among others, yet your department actually slid backward from a D to an F. What happened and what can we expect to see happen next year?

Mr. WEEMS. Well, Mr. Chairman, I work for Secretary Thompson, and on this scale, there's only one passing grade, and NRC has it.

Yes, we did slide backward, and our goal is an A, and the Secretary has made that very clear to me. Last year we were scored before Secure One HHS was launched. In looking back over that report and what happened, I certainly don't want to sound like "the dog ate my homework" sort of excuse here. We do have deficiencies in HHS, but one of those deficiencies is documentation. If we had sufficient documentation for some of our procedures, our grade would have been higher. So there may have been a difference between the way that we are evaluated and the way that security works in the real world.

Having said that, we are striving to do as you have said, which is to institutionalize security into HHS, largely through the budget process, but also through clear lines of responsibility emanating from my office through our various operating divisions, so we'll make it clear who is responsible for what and along what time lines.

Mr. PUTNAM. Your budget has, I believe, increased substantially since the creation of the Department of Homeland Security; is that correct?

Mr. WEEMS. Yes, just a few items went to the Department of Homeland Security, but our budget for bioterrorism, which is a substantial piece, has gone from about $300 million to about $4.1 billion in the fiscal 2005 budget.

Mr. PUTNAM. Since your profile has been raised as a result of the Department's role in the anthrax investigation and ricin, and your Secretary's launch of his war room, as well as just the increased awareness in the nature of biothreats, have the attempted hacks and attacks on your information systems increased as your profile has been raised?

Mr. WEEMS. We have noticed some increase there.

One of the things that I think would be helpful, and I believe that this subcommittee has pointed out, would be a uniform standard for reporting those. As you know, HHS reported a substantial number of incidents, but since they're measured inconsistently across all departments, it's difficult for us to be able to determine our posture with respect to other agencies which may report one, for instance, over a year.

With the growth of our bioterrorism efforts, that is a place where we have been very careful to make sure that we have sufficient security, and not just cybersecurity but also physical security. You can see that at the NIH campus in Bethesda and the CDC campus down in Atlanta.

Mr. PUTNAM. Mr. Rush, now that FISMA is permanent and we're working on our second year, using the same scoring standards, do you anticipate a change in resources allocation either for the purpose of contracting, or a shift in staffing similar to that, that was caused by the CFO Act that would allow you to have the tools you need to be in compliance with FISMA?

Mr. RUSH. We're going to have the tools that we need this year because the Deputy Secretary is taking over supervision of the CIO operations and there's going to be a concerted effort to see some improved performance from management. It has to be matched by what we do not only in the content of that work, but in the timeliness of the work. So I think we're in good shape for 2004.

We're going to be meeting as early as next week to try to bring that to conclusion. But long term, I think we have to come to grips with jobs that are process jobs for IGs. These are compliance-type jobs for IGs. And while I'm not here to speak on behalf of that community, as one who's been in that community a long time, we can meet the deadline, but we need to begin to rationalize some things.

I, for one, complained to OMB that the timing didn't make a lot of sense. Notwithstanding our resources, it made no sense to me to be reporting in September on FISMA when we operate on a fiscal year that ends September 30 and we have financial reporting that started as early as November 15. Trying to bring some of these deadlines and due dates into sync makes a lot more sense to folks like me, who have to audit.

Second, the act didn't have a date; it merely said that OMB could establish a date. So we thought it fair for them in the future to consider a different reporting date than September 15. That's not a date that's particularly useful for management, by the way. It's completely out of context with their own mission and performance reporting.

So there's a lot to be done as we look out at FISMA 2005–2006. But for 2004, I think we're just going to knock along and get the job done.

At Treasury, I think you'll see some improved performance. I'm very impressed with Deputy Secretary Sam Bodman. He's only been in the Department about 2 months. He comes to us from the Commerce Department where he had real impact on the Department's operation, and we hope that he'll bring that to Treasury.

Mr. PUTNAM. Those are very interesting suggestions, yours on the reporting deadlines and Mr. Weems's suggestion on the consistent measurements of incidents.

Mr. Merschoff, do you have any thoughts on ways that we can improve what is measured, how it is measured, is it relevant, is the benchmark appropriate? Your thoughts?

Mr. MERSCHOFF. I agree with Mr. Weems. It's important to be able to compare your organization to other organizations to benchmark to understand if you're doing something substantially different that needs to be addressed. In our case, we reported 67,000 incidents last year to FedCirc. Some report one or two or three, and so it's absolutely impossible——

Mr. PUTNAM. Do you know who? HUD had only one attempted—only one incident. So I guess nobody's interested in breaking into HUD's information security or something. It would be quite remarkable.

Mr. MERSCHOFF. But if we're to get better, the CIO Council, working together with benchmarking across the entire spectrum of what we do, will help us realize where we're performing at a level less than the rest of the government on the way to seek help and also to provide that help to others.

Mr. PUTNAM. Mr. Corts, you're relatively new to this ball game. You came from the academic world. What are your thoughts on the benchmark and the appropriateness of the standards.

Mr. CORTS. Well, I would certainly agree with the consistency issue and, I think, the definitional issue. You have to get a clear understanding that everybody is talking the same language and comparing apples to apples. And I think—you know, I do think this is still a pretty nascent operation, and as it matures—and I think it was the language that Karen Evans was using—we're going to see things will coalesce better in terms of agreement about terms and manners of reporting and so forth, which will be to the benefit of all of us from the point of view of benchmarking. And in the accreditation work that I'm familiar with from academe, those are crucial, just a crucial part of the accreditation process.

Mr. PUTNAM. What's your deadline for your budget submission—I guess Mr. Rush, since you raise the issue of deadlines. My understanding is that OMB set the date for FISMA reporting to coincide with your budget submissions; is that correct?

Mr. RUSH. That may have been their judgment. It did not match with the submission. The submission process for the fiscal year actually spilled over into late October. We had reclama as late as November. The appeals to the President did not occur until December, as I recall, this past year and the President submitted his budget on February 1st.

Mr. PUTNAM. So what——

Mr. RUSH. So I do not see a connection between the budget process and FISMA reporting, if there's supposed to be one, and I'm not going to object to that. It does not give September 15 a particular value as a day.

Mr. PUTNAM. What date would be more appropriate in your view?

Mr. RUSH. We invest so much in financial systems reporting because of the Chief Financial Officers Act and GMRA, that it would be useful, if we were able to tie our FISMA reporting, which often relies on the EDP control audit work in the big financial systems, to do it at about the same time or within 30 days.

And I'm not making that recommendation for all IGs. I can say from Treasury's standpoint, if we could rely on the important IT audit work that is part of our consolidated financial statement audit, we would be able to get that report out and I think you'd get a better product. It's late, but I think you will get a better product.

Mr. WEEMS. Mr. Chairman, perhaps I can answer that at least from the standpoint of the HHS. Our budget deliberations, internally at least, inside the Office of the Secretary, typically are in July. So if we were in possession of the FISMA report in advance of July, we certainly could consider that as part of our budget deliberations.

Typically, August is spent trying to complete the necessary documentation to send in a budget to OMB, which is due usually right after Labor Day. So, in fact, I believe this year we had submitted our budget document to OMB before the FISMA report was complete.

Also, as Mr. Rush has noted, we were in similar throes of trying to complete our own audit, which took an awful lot of my time and the time of other departmental officials, especially the last quarter of the fiscal year and the foregoing 45 days, to get to the November 15 audit report date consumes an awful lot of time on the financial side and a tremendous amount of the leadership's time as well.

So I would say, from our standpoint, the FISMA report being available on a contemporaneous basis in June or May would be really important to our budget process.

Mr. PUTNAM. Well, that's very helpful and I appreciate your suggestions on ways that we can perhaps make FISMA even more meaningful, the information from the report more actionable.

But three of the four of you don't have a whole lot of credibility on making recommendations for changes to this thing, and some folks have figured out how to do it. It's really kind of a unique thing to government that there is this kind of flexibility. There are a lot of things going on in February and March, but you still have to pay your taxes on April 15. You can get the extension, you get the extension, but you've still got to pay the man. And people have to file all kind of reports to be in compliance with the government.

And your agencies, your departments and all the other ones, are not nearly as understanding as OMB has been and, frankly, even as Congress has been about people who just don't do it, or they do it 3 months late or they do it whenever they get around to it. So we'll take these under advisement.

But the last thing I want to do, I do not want to cutoff my nose to spite my face and avoid making solid, common-sense changes that you guys recommend that might make sense; I do not want to ignore good suggestions. But what I do not want is for there to be yet another reason why people are not scoring particularly well because we've changed the rules on them, and we have once again given them a whole new set on the standards by which they're supposed to play ball.

The one thing about this year's score is that it is the first time that we have back-to-back years that actually are comparable, apples-to-apples comparisons to really measure progress. And all the frustrations and all the timing issues and the inconsistent report-

ing issues, particularly, that relate to incidents affect everyone the same way. So, you know, the A guys are dealing with the same lack of clarity as the F guys. And so if it's off, it's consistently off throughout the government, and it's still relatively correct.

So we'll take your points under advisement as we review there.

But the last thing I want to do is provide another reason why people can come back and say, well, you know, we were all geared up for the 2004 structure, but then in 2006 you guys moved the yardsticks on us. So we would have been there, but we were prepared for the old standard.

I would give all of you the opportunity to provide any closing remarks and then we will adjourn the hearings. So, Mr. Weems, if you would like to offer any thoughts, things that you would wish had come out, suggestions, we'll move on down the line.

Mr. WEEMS. Nothing else, Mr. Chairman, except we look for a better grade, and if you're looking for a responsible official in HHS, that's me. Thank you.

Mr. PUTNAM. Thank you.

Mr. MERSCHOFF. Yes, Mr. Chairman, I would like to recognize two reasons for our success. One is the computer security staff. They're dedicated, they're motivated, they're competent, they're capable and they're the engine behind our success.

The second is the Office of Inspector General. We have a good and productive partnership, a dynamic tension with that group where we can disagree with them, they can criticize us, we listen to each other and recognize that sometimes we're wrong and sometimes we're right; and I think that's helped us a lot in terms of improving.

That concludes my remarks.

Mr. PUTNAM. Thank you very much.

Mr. Rush.

Mr. RUSH. I just want to be sure that I close by making clear to you that the problem with timeliness was the problem of the Office of Inspector General. It was not the Treasury Department. It was not IRS. It was not my partner, the Treasury Inspector General for Tax Administration. Each of those three partners of mine did their work on time, met the standard and got their work product to OMB. The only delinquency at Treasury came out of my office, and I regret that.

Mr. PUTNAM. Thank you for your candor and for your suggestions as well. They were good.

Mr. Corts.

Mr. CORTS. Back to your point about the time that you do this and the consistency and so forth, there is a lot of value, I think, in being able to, even if the date might not be where everybody wants it, you keep that date, you keep the standard so you've got the measurement.

Going forward 2 years in a row now, it would be great to see another year. What's the right time? I'm sure we could debate that around, because it could serve all of us; different times would serve all of us, maybe any one of us better than another date. But I do think there's a lot of value in consistency, and I know we look for that in terms of benchmarking.

Finally, Mr. Chairman, we just want you to know that the Department of Justice considers this to be of the highest priority to us, and we fully intend to improve our mark. And we intend to be here and look forward to being here and giving you a better report in the future.

Mr. PUTNAM. Thank you very much.

I want to thank all of our witnesses from both panels for their contribution to our oversight efforts. As we face almost daily reports of the IT vulnerabilities, the Federal Government really must be a shining example of IT security.

I also want to mention that I will be meeting with the Federal CIO Council again to express my commitment to this issue as well as to hear their feedback on why so many agencies have not produced better progress, and perhaps to solicit more suggestions, as you have provided, on ways that we can improve the process.

In the event that there may be additional questions we did not have time for today, the record will remain open for 2 weeks for submitted questions and answers.

Thank you very much. The subcommittee is adjourned.

[Whereupon, at 3:42 p.m., the subcommittee was adjourned.]

[The prepared statement of Hon. Wm. Lacy Clay and additional information submitted for the hearing record follow:]

STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
INFORMATION TECHNOLOGY MANAGEMENT

MARCH 16, 2004

Thank you Mr. Chairman, and I thank the witnesses for taking their time to be with us today. I look forward to the discussion today.

The federal government will spend approximately $60 billion on information technology in fiscal year 2004. These investments, however, rarely meet their full potential due to the absence of strategic planning and adequate performance measures throughout the IT procurement and implementation process. As the federal government continues to shift its attention towards outcome related measures when determining resource allocations in the budget process, it goes without saying that inadequate oversight of IT investments will have a domino effect of negative performance outcomes throughout the agency community.

Of particular concern to me is a lacking of consistent agency oversight efforts for IT investments, particularly in cases where Congress statutorily prescribed certain provisions, such as the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996. Whether the cause is due to inadequate agency leadership or the lack of appropriate and updated strategic and performance measures, the benefits associated with IT upgrades are not

being realized. These are not new requirements, and the agencies are failing to effectively modernize their IT systems in their absence.

In addition to statutory requirements, OMB shares in the responsibility to adequately assist and provide guidance to the agencies so they may be in compliance with the law. Thus, I was pleased to read GAO's recommendations for OMB to further assess the avenues in which annual performance reporting requirements can be enhanced by the inclusion of more detailed information concerning major IT acquisition programs.

As I have said during previous hearings on related issues, the use of technology in the federal government has not always provided the benefits originally envisioned. While the findings contained in the GAO report before us this morning are not surprising, they should sharpen our focus on deriving greater value from what is an enormous annual investment during times of limited resources.

Again, thank you Mr. Chairman, and I ask unanimous consent that the full text of my remarks be included in the record.

United States General Accounting Office
Washington, DC 20548

April 2, 2004

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Subject: *Information Security: Responses to Posthearing Questions from March 16, 2004, "Information Security in the Federal Government: One Year into the Federal Information Security Management Act"*

As requested in your letter of March 17, 2004, this letter provides our responses for the record to the questions you posed to us following the March 16 hearing. At that time, we discussed efforts by federal departments and agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) to implement requirements of the Federal Information Security Management Act of 2002 (FISMA).[1] The following responses to your questions are based on our written statement for this hearing.[2]

1. *After four years of performance measures, are there changes that you would recommend in those measures?*

As we emphasized in our written statement, the current FISMA performance measures focus on implementation of statutory requirements. The periodic reporting of these measures and related analysis can provide valuable information on the status and progress of agency efforts to implement effective security management programs, thereby assisting agency management, OMB, and the Congress in their management and oversight roles.

Further, in our written statement we noted several opportunities to improve the usefulness of such performance information as indicators of both governmentwide and agency-specific progress in implementing information security requirements. Specific areas we highlighted included:

- providing greater assurance on the reliability and quality of reported performance measures through such means as inspector general (IG) reviews;

---

[1] *Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002,* P.L. 107-347, December 17, 2002.
[2] U.S. General Accounting Office, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements,* GAO-04-483T (Washington, D.C.: March 16, 2004).

- reporting performance measurement data according to the relative importance or risk of the systems, such as the risk categories recently issued by NIST;[3] and
- refining performance measures to provide more useful information about the quality of agency processes.

In its fiscal year 2003 FISMA report, OMB acknowledged the need for FISMA reporting to mature, and is focusing on areas including (1) evolving the information technology (IT) security performance measures to move further beyond status reporting to also identifying the quality of the work done, and (2) further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes, such as remediation of information security weaknesses and intrusion-detection and reporting.[4]

Analysis of problems identified in agency FISMA reports and other sources can target areas where reported FISMA information could be improved, through enhanced performance measures and/or through independent IG evaluations. For example, our ongoing review and IG fiscal year 2003 FISMA evaluations identified deficiencies in the certification and accreditation process, such as lack of control testing and outdated risk assessments.[5] Additional performance data reported on key aspects of certification and accreditation would provide better information with which to assess whether they were performed consistently. Also, OMB could require targeted IG reviews of agency certification and accreditation processes to identify any related weaknesses. Based on identified problems, other potential areas for additional performance information and/or targeted review include the quality of certain agency information security processes, such as detecting, reporting, and responding to security incidents, and confirming that software patches have been tested and installed in a timely manner.[6]

Additionally, as agencies report increasing compliance with basic performance information, such measures can evolve to capture more sophisticated or refined information. For example, although most agencies are reporting that they have implemented procedures for overseeing security at contractor sites, information about the nature and extent of contractor procedures could assist in assessing the quality of such procedures. Additional information could be obtained, for instance, on whether specific security requirements for contractor-provided services had been

---

[3]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199, December 2003.

[4]Office of Management and Budget, *FY 2003 Report to Congress on Federal Government Information Security Management*, March 1, 2004.

[5]OMB's policy for federal information security requires that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

[6]A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered. Patch management is the process of effectively applying available patches.

formally agreed to. OMB used a similar approach in its fiscal year 2003 FISMA reporting instructions by requesting more detailed performance information about agencies' plans of action and milestones processes to better assess their quality.[7] This approach is also consistent with NIST's security metrics guidance, which discusses how the focus of security performance metrics changes as the implementation of security controls matures toward measuring effectiveness and efficiency of implemented security controls and the impact of these controls on the organizations' missions.[8] Another area for possible refinement of performance measures relates to the ability of agencies to routinely provide security management information to manage their information security activities.

2. *Several of the witnesses suggested that changing the reporting date for FISMA to coincide with the financial reporting date would enhance reporting. Do you think that this is a good suggestion? Do you think it would ease or improve reporting?*

Any consideration of reporting dates should take several factors into account, including the ability to incorporate FISMA reporting into the agency's and OMB's budget preparation and review process, OMB's ability to meet its statutory March 1 congressional FISMA reporting date, and the ability to integrate work related to FISMA with the annual agency financial audits.

Neither the prior Government Information Security Reform provisions (commonly known as GISRA[9]) nor FISMA established a specific date for when agencies are to report. However, beginning with GISRA reporting, OMB has required agencies to submit their reports concurrently with their budget submissions in the mid-September time frame. For example, last year's FISMA reports were due to OMB by September 22, 2003. Further, neither GISRA nor FISMA established an effective date as of when the information is to be prepared.

In its fiscal year 2003 FISMA report to the Congress, OMB reported that it uses the FISMA information to make funding decisions. For example, OMB reported that it used the information to review whether the agencies appropriately budgeted for remediation of security weaknesses in their fiscal year 2005 budgets and in prioritizing fiscal year 2004 funding decisions. OMB directed agencies with significant information and systems security weaknesses to correct weaknesses in operational systems prior to spending fiscal year 2004 IT development or modernization funds. If additional resources are needed to resolve those weaknesses, agencies were to use those fiscal year 2004 IT funds originally sought for new development.

---

[7]Required for all programs and systems in which an IT security weakness has been found, a plan of action and milestones (POA&M) lists the weaknesses and shows estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

[8]National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems,* Special Publication 800-55 (July 2003).

[9]*Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001,* P.L.106-398, October 30, 2000.

Additionally, agencies were expected to tie their plans for correcting information security weaknesses to their system budget requests through IT business cases, as required in OMB budget guidance (Circular A-11). Consequently, completing the agency's FISMA assessments in time for consideration in the preparation of agency budget requests would be desirable.

Ideally, the work on information security for FISMA and for the financial statement audits would be integrated. As we have previously reported, at some agencies, financial systems comprise virtually all major systems, while others, such as DOD and Justice, operate a significant number of nonfinancial systems. Agency fiscal year 2004 financial statement audit reports are due November 15, an acceleration from previous February and March due dates for fiscal years 2002 and 2001, respectively. Assessments of information security controls in a financial audit can be performed as of an interim date in combination with appropriate procedures to update the assessment through the end of the fiscal year. For example, information security assessments could be completed earlier in the fiscal year (such as at the end of June or July), and updated through the end of the year using appropriate procedures.

Regardless of the reporting date, consideration should be given to ensuring consistent reporting periods for the agency reviews and IG independent evaluations, to provide better comparability in results. Our analyses of fiscal year 2003 IG FISMA evaluation reports identified instances in which the IGs were unable to review agency-reported data because the data were not available at the time of their work. For example, one IG noted that the agency had completed certification and accreditation for two mission-critical systems after the conclusion of its audit and, thus, did not evaluate whether the certification and accreditation process had effectively identified and mitigated significant security risks for those systems. In another example, an IG reported that data on the agency's fiscal year 2003 security training and budget information on IT investments were not available in time for review, and that these data would be reviewed as part of its next FISMA audit cycle.

3. Now that FISMA is permanent, do you foresee a ramping up of resources, both staffing and contracting, similar to what was caused by the CFO Act?

The information security requirements in FISMA consolidate separate requirements previously established in law and consistent with existing information security guidance issued by OMB[10] and NIST,[11] as well as audit and best practice guidance issued by us.[12] However, as we highlight in our written statement, agency-reported performance data for fiscal year 2003 showed that there were agencies where less

[10]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[11]Numerous publications made available at http://www.itl.nist.gov/, including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.

[12]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

than half of the systems met requirements for risk assessments, security plans, certifications and accreditations, tested security controls, and tested contingency plans. Further, in its March 2004 report to the Congress, OMB noted that too many legacy systems continue to operate with serious weaknesses, and that there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses is funded prior to proceeding with new development. Depending on the effectiveness of an agency's information security program, focusing agency or contractor resources on correcting such weaknesses may be required in order to achieve significant progress, particularly in implementing potentially resource-intensive requirements. In addition, it remains to be seen what effect new FISMA requirements, such as implementing mandatory minimum security controls, will have on agency resource needs. However, we believe that establishing effective agencywide information security programs that routinely implement and monitor FISMA requirements can minimize the need for additional resources.

4. *Do [you] foresee a need for standardized guidance for the Inspectors General to ensure that FISMA audit work is reliable and consistent?*

We believe that overall guidance for use by the IGs in conducting their independent FISMA evaluations could help to produce more consistent results, particularly in helping to ensure the reliability and quality of agency-reported performance measures and the completion of corrective actions. For example, as we noted in our written statement, OMB did not require the IGs to validate agency responses to the performance measures, but did instruct them to assess the reliability of the data for the subset of systems they evaluate as part of their independent evaluations. Not all IGs consistently addressed this instruction, but some IG evaluations did identify problems with data reliability and quality that could affect agency performance data. One such case was the performance measure on the number of agency systems authorized for processing after certification and accreditation, in which six IGs indicated different results than those reported by their agencies, for reasons such as out-of-date certifications and accreditations (systems are to be reaccredited at least once every 3 years). The IGs have, however, recognized the need to develop standardized guidance. We have begun to work with a FISMA working group of the Federal Audit Executive Council and, among other things, have discussed the issue of an evaluation methodology or guidance for the IG community.

NRC'S RESPONSE TO QUESTIONS CONTAINED IN A LETTER FROM THE HONORABLE ADAM H. PUTNAM CHAIRMAN, SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS UNITED STATES HOUSE OF REPRESENTATIVES DATED MARCH 17, 2004

Question 1. **Getting senior program officials to take accountability for the mission systems they control is a recurring theme in OMB's FISMA report. Have you found the certification and accreditation process which requires the program official to sign off on the risk level any help with this?**

Answer: Yes, the certification and accreditation process has helped to get senior program officials to take accountability for the mission systems they control. This is accomplished by providing high level visibility to the risk level associated with mission systems which may not have been identified outside of the certification and accreditation process. This visibility provides senior program officials with an awareness of the risks associated with mission systems, the opportunity to follow up on actions being taken to control risks, and provides senior management with leverage to ensure senior program officials are taking the appropriate steps to control these risks.

Question 2. **How does your agency ensure that the information you report for FISMA accurately reflects the status and quality of information security at your agency?**

Answer: NRC accomplishes this through several mechanisms. The NRC has a dedicated Computer Security staff that performs oversight activities, including an independent review of all security documentation, capital planning information, system penetration testing, and innovative ideas such as independent security control evaluation to ensure accurate and complete information. The agency head and the CIO utilize a central tracking system to track all system information such as the status of security plans, security testing, system weaknesses and corrective actions, and all other security activities associated with systems security certification and accreditation. The agency head and the CIO ensure that new systems cannot be placed into operation, and major system upgrades cannot be completed, until they have completed the security activities and milestones required to attain systems security accreditation. In addition, the NRC's Office of Inspector General performs an independent assessment of the overall computer security program on an annual basis.

Question 3. **Several witnesses testified that moving FISMA reporting to align with financial reporting would be helpful. What are your thoughts on this proposal?**

Answer: NRC believes the date should remain the same to ensure the ability to compare results from year to year.

Enclosure

ANSWERS BY ASSISTANT ATTORNEY GENERAL FOR ADMINISTRATION PAUL R. CORTS TO QUESTIONS FOR THE RECORD FROM HEARING ON "INFORMATION SECURITY IN THE FEDERAL GOVERNMENT: ONE YEAR INTO THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT" HOUSE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS, AND THE CENSUS COMMITTEE ON GOVERNMENT REFORM MARCH 16, 2004

1. **You point out in your testimony the decentralized structure of Justice. How has the Agency granted the CIO authority to deal with those different components? How is compliance with his policies enforced at the Agency?**

In the past, the Department of Justice (the Department) operated in a very decentralized environment. Through the Attorney General's leadership and vision, we have become a more centrally-coordinated Department, including our information technology (IT) programs. This has had a positive impact on our IT efforts.

Greater IT coordination department-wide has significantly improved through the implementation of organizational changes. First, the Department clarified that the Chief Information Officer (CIO) reports directly to the Attorney General for the duties and responsibilities identified by the Clinger-Cohen Act. The CIO also serves as the Deputy Assistant Attorney General (DAAG) for Information Resources Management, and is a vital part of the Department's management team. This ensures that the CIO routinely coordinates IT initiatives and programs through the office of the Assistant Attorney General for Administration, who serves as the Department's Chief Financial Officer and Procurement Executive.

Second, the CIO oversees all IT programs throughout the Department. The CIO oversees and advises component heads on the selection of their CIOs. This opportunity ensures high quality, Department-wide coordination of IT.

Third, the CIO developed and implemented IT policy, standards, and guidelines to provide increased oversight of component IT programs and projects. This ensures compliance with Departmental IT policies, priorities and initiatives. Performance metrics relating to the Federal Information Security Management Act (FISMA) are tracked on a by-component basis. The CIO and Deputy CIO for IT Security monitor component progress towards meeting these performance measures. The CIO meets with program officials and component CIOs regularly to ensure compliance with Departmental IT policies and initiatives.

Fourth, the CIO's role as the DAAG for Information Resource Management offers and ensures his participation on the management leadership team. This enables him to intercept IT matters that may attempt to progress without his review, coordination, and approval.

In conclusion, like most agencies we have implemented a number of new IT security policies and processes designed to further protect our systems and networks. Accountability and responsibility are critical to our successful remediation of identified vulnerabilities and weaknesses. Our CIO and key members of our IT Security staff will be meeting with your staff in the upcoming weeks to further discuss our IT security initiatives and the progress we have achieved within our program. I believe that when you review the record of accomplishments in IT security achieved this fiscal year, you will see that the Department has made significant strides in order to overcome past deficiencies and ensure a secure IT environment for the Department.

2. Getting senior program officials to take accountability for the mission systems they control is a recurring theme in OMB's FISMA report. Have you found the certification and accreditation process which requires the program official to sign off on the risk level any help with this?

Yes, senior program officials are accountable, and are becoming more aware of the importance of IT security within their programs through the certification and accreditation process. Additionally, the Department established a certification and accreditation help desk that was designed to assist program officials and information system security officers with the resources for planning, implementing, and maintaining security throughout the system development life cycle and the certification and accreditation process.

3. How does your agency ensure that the information you report for FISMA accurately reflects the status and quality of information security at your agency?

The DOJ ensures that the FISMA information is accurate by increasing the resources committed to IT security and by making organizational changes that strengthen personnel resources dedicated to IT. We have added a new security administrator to our IT personnel staff who has implemented new IT security policy guidance and 17 IT security standards based upon guidance from the National Institute of Standards and Technology. The new security administrator oversees an administrative council of staff that is responsible for the FISMA reporting. We are currently in the process of implementing an automated tool to track the status of security within a system in order to provide for consistent and accurate FISMA reporting across the Department.

4. Several witnesses testified that moving FISMA reporting to align with financial reporting would be helpful. What are your thoughts on this proposal?

The current FISMA reporting is acceptable and aligns with the budget process and reporting to OMB. The personnel who respond to these FISMA queries are separate and distinct from those who are reporting the Department's financial data. The Department believes that IT security must be maintained and continuously evaluated throughout the year.